СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

РАБОЧАЯ ИНСТРУКЦИЯ

РИ 6.5-2

Положение по защите персональных данных

Регистрационный номер документа	
Структурное подразделение	
Уполномоченный по качеству	
Дата получения	

Комсомольск-на-Амуре
2015

РАБОЧАЯ ИНСТРУКЦИЯ

Система менеджмента качества **ПОЛОЖЕНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**	**РИ 6.5-2** **Введена впервые**

СОГЛАСОВАНО

Первый проректор

_____ И.В. Макурин

«28» января 2015 г.

Начальник ИТ-Управления

_____ Е.Б. Абарникова

«28» января 2015 г.

Начальник организационно-правового управления

_____ Н.А. Лашкина

«28» января 2015 г.

УТВЕРЖДАЮ

Ректор университета

_____ Э.А. Дмитриев

«29» января 2015 г.

Комсомольск-на-Амуре
2015

Введена приказом № 39а-О от 29.01.2015

Содержание

1 Назначение и область применения

1.1 Назначение

Настоящее Положение определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных ФГБОУ ВО «КнАГУ». Положение определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации. (**Изм. № 1, 2**)

1.2 Сфера действия

Положение распространяется на следующие объекты защиты: обрабатываемые в ФГБОУ ВО «КнАГУ» персональные данные субъектов персональных данных, технологическая информация, схемы технологических процессов обработки, программно-технические средства обработки, средства защиты персональных данных, каналы информационного обмена и телекоммуникации, объекты и помещения, в которых размещены компоненты информационных систем обработки персональных данных. (**Изм. № 1, 2**)

1.3 Область применения

Настоящее положение должны использовать в своей работе администраторы безопасности, сотрудники ИТ-Управления, сотрудники ФГБОУ ВО «КнАГУ», осуществляющие обработку персональных данных субъектов персональных данных и/или имеющих доступ в помещения обработки и/или хранения носителей персональных данных. (**Изм. № 1, 2**)

2 Нормативные ссылки

Настоящее положение разработано в соответствии со следующими нормативными документами:

Конституция Российской Федерации.

Трудовой кодекс Российской Федерации.

Кодекс об административных нарушениях Российской Федерации.

Гражданский кодекс Российской Федерации.

Уголовный кодекс Российской Федерации.

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

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

Постановление Правительства «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687.

Постановление Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах

персональных данных» от 1 ноября 2012 г. № 1119.

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

Приказ ФСБ России «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» от 10 июля 2014 г. № 378.

3 Термины, определения, сокращения

3.1 Термины и определения

В настоящем положении применяются следующие термины с соответствующими определениями:

Администратор безопасности информационной системы обработки персональных данных – штатный сотрудник университета, назначенный приказом руководства университета, осуществляющий проведение и контроль мероприятий по обеспечению безопасности персональных данных, методическое руководство работой пользователей информационной системы персональных данных и отвечающий за обеспечение устойчивой работоспособности элементов информационной системы персональных данных и средств защиты при обработке персональных данных.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый

программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – возможность за приемлемое время получить требуемую информационную услугу.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Инцидент – некоторое происшествие, связанное со сбоем в функционировании элементов информационной системы персональных

данных, предоставляемых пользователям системы, а так же потерей защищаемой информации. Инцидент может произойти в результате непреднамеренных действий пользователей, преднамеренных действий пользователей и третьих лиц, нарушения правил эксплуатации технических средств, в результате возникновения внештатных ситуаций и/или форс-мажорных обстоятельств.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией,

нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или 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.

Носитель персональных данных – материальный объект (бумажный или электронный) содержащий персональные данные.

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

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

Помещение персональных данных – помещение, содержащие носители персональных данных.

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

Работник (сотрудник) – физическое лицо, состоящее в трудовых

отношениях с работодателем.

Работодатель – ФГБОУ ВО «Комсомольский-на-Амуре государственный университет», выполняющий функции оператора персональных данных. (**Изм. № 1, 2**)

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

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

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Руководство — Ректорат университета.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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.

Университет – ФГБОУ ВО «Комсомольский-на-Амуре государственный университет». (**Изм. № 1, 2**)

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

3.2 Сокращения

В настоящем положении применяются следующие сокращения:

АБ – Администратор безопасности ИСПДн;
АВПО – антивирусное программное обеспечение;
АРМ – автоматизированное рабочее место;
ИСПДн – информационная система персональных данных;
ЛВС – локальная вычислительная сеть;
МЭ – межсетевой экран;
НСД – несанкционированный доступ;
ОС – операционная система;
ПДн – персональные данные;
ПО – программное обеспечение;
ППДн – помещение, содержащее носители персональных данных;
РФ – Российская Федерация;
СЗИ – средства защиты информации;
СЗПДн – система (подсистема) защиты персональных данных;
УБПДн – угрозы безопасности персональных данных;
RAID – технология виртуализации данных, которая объединяет несколько дисков в логический элемент для избыточности и повышения производительности.

4 Ответственность

4.1 Работники университета, имеющие доступ к ПДн субъектов ПДн, несут ответственность в соответствии с законодательством РФ за нарушение режима защиты, обработки и порядка использования ПДн.

4.2 Работники университета, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн субъектов ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

4.3 Контроль за выполнением норм, регулирующих получение, обра-

ботку и защиту ПДн субъектов ПДн возлагается на руководство университета, начальника ИТ-управление, руководителей структурных подразделений университета, в которых осуществляется обработка ПДн.

5 Общие положения

5.1 СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

5.2 Безопасность персональных данных достигается путем исключения 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.

5.3 Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии. Эти меры призваны обеспечить конфиденциальность информации, целостность информации, доступность информации.

6 Построение системы защиты персональных данных

6.1 Построение СЗПДн возлагается на ИТ-Управление.

6.2 При построении СЗПДн ответственные сотрудники ИТ-Управления и администраторы безопасности должны использовать следующие принципы:

– законность – осуществление защитных мероприятий и разработка СЗПДн в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции;

– системность – учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн;

– комплексность – согласованное применение разнородных средств

при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

– непрерывность защиты – рассмотрение защиты ПДн как непрерывного целенаправленного процесса, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн;

– своевременность – разработки и эксплуатация СЗПДн параллельно с разработкой и развитием ИСПДн для упреждающего характера мер обеспечения безопасности ПДн;

– совершенствование – постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области;

– персональная ответственность – возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий;

– минимизация полномочий – предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено»;

– гибкость – возможность варьирования уровнем защищенности, без нарушения процесса нормального функционирования ИСПДн;

– простота применения – СЗПДн должна быть интуитивно понятна и проста в использовании не требующая значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей;

– специализация – возможность привлечение к разработке средств и реализации мер защиты информации специализированных организаций, имеющих опыт практической работы и необходимые лицензии;

– контроль – возможность контроля за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты, охватывающего как несанкционированные, так и санкционированные действия с целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн.

6.3 При построении СЗПДн ответственные сотрудники ИТ-Управления и администраторы безопасности должны использовать следующие меры защиты:

– программно-аппаратные средства защиты ПДн – использование различных устройств и специальных программ, входящих в состав ИСПДн

и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты. К данным средствам относятся средства защиты от несанкционированного доступа, средства защиты с модулем доверенной загрузки, средства криптографической защиты, межсетевые экраны, антивирусные средства защиты, средства оперативного контроля и регистрации событий безопасности;

– правовые меры защиты – действующие законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей;

– административные меры защиты – меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации;

– физические меры защиты – применение механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

7 Обязанности администратора безопасности

7.1 АБ обязан знать и выполнять требования действующих нормативных и руководящих документов, перечисленных в разделе 2 данного Положения, а также руководства по эксплуатации СЗИ, входящих в состав СЗПДн и иных нормативно-правовых и административных документов в области защиты персональных данных в рамках своей компетенции.

7.2 АБ должен обеспечивать контроль за установкой, настройкой и своевременным обновлением сотрудниками ИТ-Управления элементов ИСПДн:

– программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);

– аппаратных средств;

– аппаратных и программных средств защиты.

7.3 АБ должен контролировать работоспособность элементов ИС-

ПДн и ЛВС в соответствии с техническими условиями эксплуатации соответствующих систем.

7.4 АБ должен осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, копий носителей персональных данных.

7.5 АБ обязан обеспечивать функционирование и поддерживать работоспособность средств защиты информации в рамках возложенных на него функций.

7.6 В случае отказа работоспособности средств защиты информации, АБ должен принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

7.7 АБ должен проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

7.8 АБ должен обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

7.9 АБ обязан информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

7.10 АБ имеет право требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

7.11 АБ обязан присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими людьми и/или организациями.

7.12 АБ должен совместно с назначенными сотрудниками принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.

8 Обеспечение непрерывной работы

8.1 Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, и контроль обеспечения мероприятий по предотвращению инцидентов безопасности является АБ ИСПДн.

8.2 Для обеспечения непрерывной работы и восстановления ресурсов при возникновении инцидентов должны быть приняты технические и организационные меры. Ответственного за реализацию соответствующих мер определяет руководство университета.

8.2.1 К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов:

– системы жизнеобеспечения;

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных;

– системы контроля физического доступа.

8.2.1.1 Системы жизнеобеспечения ИСПДн включают:

– пожарные сигнализации и системы пожаротушения – все помещения, в которых размещаются сервера ИСПДн, должны быть оборудованы средствами пожарной сигнализации;

– системы вентиляции и кондиционирования – для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха;

– системы резервного питания – Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

8.2.1.2 Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение ПДн, сотрудниками ИТ-Управления должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

8.2.1.3 Для резервного копирования и хранения данных сотрудниками ИТ-Управления должны использоваться соответствующие системы, обеспечивающие хранение защищаемой информации на материальном носителе: жесткий диск, flash-накопитель, компакт-диск и т.п.

8.2.2 К организационным мерам обеспечения непрерывной работы и восстановления относится резервное копирование.

8.2.2.1 Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемых ПДн – не реже раза в месяц;

– для технологической информации – не реже раза в год;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – каждый раз при внесении изменений в эталонные копии (выход новых версий).

8.2.2.2 Данные о проведение процедуры резервного копирования,

должны отражаться в специально созданном журнале учета.

8.2.2.3 Носители, на которые произведено резервное копирование, должны быть пронумерованы.

8.2.2.4 Носители должны храниться в несгораемом шкафу или сейфе.

8.2.2.5 Ответственным за осуществление резервного копирования и хранения данных является администратор ИСПДн и/или иное лицо назначенное руководством университета и/или руководителем ИТ-Управления.

8.3 В случае наступления инцидента, в кратчайшие сроки, не превышающие одного рабочего дня, АБ совместно с назначенными сотрудниками предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

9 Физическая охрана помещений персональных данных

9.1 ППДн в нерабочее время должны быть закрыты на ключ и сданы под охрану.

9.2 В ППДн имеют допуск только лица, допущенные в приказом руководства университета к обработке ПДн. Возможность неконтролируемого проникновения или пребывания в этих ППДн посторонних лиц должна быть исключена. Ответственным за выполнения требований данного пункта является ответственный за данное ППДн.

9.3 По окончании рабочего дня ППДн запирает и сдает под охрану работник, имеющий право доступа в Помещение.

9.4 В начале рабочего дня работник, имеющий право доступа в ППДн, перед вскрытием ППДн проверяет целостность и исправность сигнализации и дверных запоров. В случае обнаружения нарушений, указывающих на возможность проникновения в ППДн посторонних лиц, работник ППДн не вскрывает, а о случившемся незамедлительно сообщает АБ, который в свою очередь незамедлительно ставит в известность свое руководство и в случае необходимости составляет акт.

9.5 При срабатывании охранной сигнализации, извещающей о несанкционированном доступе или попытке доступа в ППДн АБ незамедлительно должен прибыть к входной двери ППДн, выяснить причину срабатывания сигнализации и поставить об этом в известность непосредственного руководителя.

10 Разработчики

Данный документ разработали:

Начальник ИТ-Управления — Е.Б. Абарникова

Ведущий специалист по информационной безопасности ОССА ИТ-Управления — Д.С. Магола

Введена приказом № 39а-О от 29.01.2015

Лист регистрации изменений

	Номер приказа, дата утверждения изменений	Количество страниц изменения	Дата получения изменения	Подпись уполномоченного по качеству
1	№ 100-О от 15.03.2016	-	15.03.2016	Короткова М.В.
2	№ 166-О от 10.04.2018	-	10.04.2018	Усова Т.И.

Введена приказом № 39а-О от 29.01.2015