АДМИНИСТРАЦИЯ ОКТЯБРЬСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ПЕРМСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

02.03.2018 № 118-266-01-05

Об утверждении отдельных документов по персональным данным в Администрации Октябрьского муниципального района Пермского края

В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", Федеральным законом от 02 марта 2007 г. N 25-ФЗ "О муниципальной службе в Российской Федерации", постановлениями Правительства Российской Федерации от 21 марта 2012 г. N 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", от 01 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",
Администрация Октябрьского муниципального района ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые:

1.1. Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в Администрации Октябрьского муниципального района Пермского края.

1.2. Инструкцию о порядке проведения разбирательств по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации в информационных системах персональных данных в Администрации Октябрьского муниципального района Пермского края.

1.3. Инструкцию работников Администрации Октябрьского муниципального района, допущенных к обработке конфиденциальной информации и персональных данных.

1.4. Инструкция пользователя по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах Администрации Октябрьского муниципального района Пермского края

1.5. Форму Журнала по учету обращений субъектов персональных данных о выполнении их законных прав в области обработки и защиты персональных данных, в том числе в информационных системах персональных данных.

1.6. Форму Журнала учета проверок юридического лица, проводимых органами государственного контроля (надзора), органами муниципального контроля.

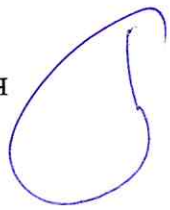
1.7. Форму Журнала проведения инструктажа по информационной безопасности.

2. Кадровому сектору Администрации Октябрьского муниципального района обеспечить ознакомление с настоящим постановлением работников Администрации Октябрьского муниципального района под подпись.

3. Руководителям структурных подразделений Администрации Октябрьского муниципального района с образованием юридического лица разработать и утвердить прилагаемые документы по персональным данным.

4. Настоящее постановление вступает в силу со дня обнародования и подлежит размещению на официальном сайте Октябрьского муниципального района.

5. Контроль за исполнением постановления возложить на заместителя главы Октябрьского муниципального района, руководителя аппарата Администрации Октябрьского муниципального района Ф.А. Поповцева.

Глава муниципального района –
глава администрации Октябрьского
муниципального района Пермского края  Г.В. Поезжаев

УТВЕРЖДЕНЫ:
постановлением Администрации Октябрьского муниципального района Пермского края
от 02.03.2018 № 118-266-01-05

Правила
оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в Администрации Октябрьского муниципального района Пермского края

I. Общие положения

1.1. Настоящие Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в Администрации Октябрьского муниципального района Пермского края (далее - Правила) определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" (далее - N 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных N 152-ФЗ.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

II. Основные понятия

2.1. В настоящих Правилах используются основные понятия:

2.1.1. Информация - сведения (сообщения, данные) независимо от формы их представления;

2.1.2. Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

2.1.3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

2.1.4. Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;

2.1.5. Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

2.1.6. Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

2.1.7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;

2.1.8. Оценка возможного вреда - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

III. Методика оценки возможного вреда субъектам персональных данных

3.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

3.2.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

3.2.2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;

3.2.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных;

3.2.4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;

3.2.5. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
3.2.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;

3.2.7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

3.2.8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

3.3. Субъекту персональных данных может быть причинен вред в форме:

3.3.1. Убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

3.3.2. Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.4. В оценке возможного вреда Администрация Октябрьского муниципального района Пермского края исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:

3.4.1. Низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

3.4.2. Средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

3.4.3. Высокий уровень возможного вреда - во всех остальных случаях.

IV. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Оператором мер

4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным за организацию обработки персональных данных в Администрации Октябрьского муниципального района Пермского края, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведенных в Приложении.

4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ N 152-ФЗ "О персональных данных", определяется лицом, ответственным за организацию обработки персональных данных в Администрации Октябрьского муниципального района Пермского края, исходя из правомерности и разумной достаточности указанных мер.

Приложение
к Правилам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в Администрации Октябрьского муниципального района Пермского края, утвержденных постановлением Администрации Октябрьского муниципального района Пермского края от 02.03.2018 № 118-266-01-05

Оценка
вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых Оператором мер

N п\п	Требования Федерального закона "О персональных данных", которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
1	порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;	Убытки и моральный вред	+	средний	В соответствии с законодательством в области защиты информации
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
2	порядок и условия применения средств защиты информации;	Убытки и моральный вред	+	средний	В соответствии с технической документацией на систему защиты ИСПД
		Целостность	+		
		Доступность			
		Конфиденциальность			

3	эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;	Убытки и моральный вред	+	высокий	Программа и методика испытаний систем защиты
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
4	состояние учета машинных носителей персональных данных;	Убытки и моральный вред			Инструкция по учету машинных носителей информации
		Целостность			
		Доступность			
		Конфиденциальность			
5	соблюдение правил доступа к персональным данным;	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
		Целостность	+		
		Доступность			
		Конфиденциальность	+		
6	наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;	Убытки и моральный вред	+	средний	Мониторинг средств защиты информации на наличие фактов доступа к ПД
		Целостность			
		Доступность			
		Конфиденциальность	+		
7	мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного	Убытки и моральный вред		низкий	Применение резервного копирования

	доступа к ним;				
		Целостность	+		
		Доступность	+		
		Конфиденциальность			
8	осуществление мероприятий по обеспечению целостности персональных данных.	Убытки и моральный вред		низкий	Организация режима доступа к техническим и программным средствам
		Целостность	+		
		Доступность			
		Конфиденциальность			

УТВЕРЖДЕНА:
постановлением Администрации Октябрьского муниципального района Пермского края
от 02.03.2018 № 118-266-01-05

Инструкция
о порядке проведения разбирательств по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации в информационных системах персональных данных в Администрации Октябрьского муниципального района Пермского края

I. Общие положения

1.1. Разбирательство по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности информации и другим нарушениям, приводящим к снижению уровня защищенности персональных данных (далее по тексту - Разбирательство) проводится с целью выяснения обстоятельств происшедшего, установления вины конкретных лиц, размера причиненного ущерба, выявления причин и условий, способствовавших изучаемому событию и применения превентивных профилактических мер в дальнейшем.

1.2. Разбирательство представляет собой процесс сбора и документирования информации, относящейся к событию и получаемой путем опроса работников Администрации Октябрьского муниципального района (далее – работники Администрации) и причастных к событию других лиц (с их согласия), располагающих информацией по данному событию, ознакомления с документами, осмотра служебных помещений, предметов, а также оценки этой информации, подготовки выводов и предложений.

II. Назначение разбирательства

2.1. Основанием для проведения Разбирательства являются ставшие известными ответственному за организацию обработки персональных данных в Администрации Октябрьского муниципального района сведения о фактах нарушений условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных и другим нарушениям, приводящим к снижению уровня защищенности персональных данных. Такие сведения могут содержаться в служебных записках руководителей подразделений, сообщениях правоохранительных органов, иных государственных, а также негосударственных структур и частных лиц.

2.2. Разбирательство назначается главой муниципального образования - главой администрации Октябрьского муниципального района путем издания распоряжения об утверждении состава комиссии по разбирательствам во главе с председателем для выполнения этой работы.

2.3. Председателем комиссии разрабатывается план проведения разбирательства, распределяются направления работы, по необходимости изучаются законодательные и другие нормативные акты по вопросам, подлежащим выяснению.

2.4. Глава муниципального района – глава администрации Октябрьского муниципального района, назначивший разбирательство, дает указание о направлении и объеме изучения события.

2.5. Работники Администрации не могут участвовать в проведении разбирательства, если они прямо или косвенно заинтересованы в его результатах.

III. Проведение разбирательства

3.1. В ходе разбирательства устанавливается:

– действительно ли имело место событие;

– обстоятельства (где, когда), при которых оно произошло;

– наличие отрицательных последствий события, характер и размер ущерба;

– причинная связь между проступком (действиями, бездействием) конкретного лица (лиц) и результатом события;

– причины и условия, способствовавшие событию (совершению проступка);

– наличие обстоятельств смягчающих или отягчающих ответственность виновного лица.

3.2. Разбирательство проводится в срок до 30 календарных дней. В случае необходимости срок разбирательства может быть продлен главой муниципального района – главой администрации Октябрьского муниципального района, назначившим разбирательство, по мотивированному обращению председателя комиссии.

3.3. Работники Администрации, которым поручено проведение разбирательства, обязаны:

– соблюдать предусмотренные законом права и интересы лиц - участников разбирательства;

– делать выводы по результатам работы комиссии только на основании фактических данных, полученных в результате разбирательства и закрепленных документально;

– своевременно докладывать главе муниципального района – главе администрации Октябрьского муниципального района, назначившему разбирательство, о выявленных нарушениях закона, причинах и условиях, способствовавших совершению проступка (правонарушения);

– в случае установления в ходе разбирательства признаков преступления немедленно доложить об этом главе муниципального района – главе администрации Октябрьского муниципального района и по его указанию направить материалы в установленном порядке в следственные (правоохранительные) органы.

3.4. Работники Администрации, которым поручено разбирательство, имеют право:

– приглашать для беседы сотрудников, а также других граждан (с их согласия), получать от них письменные объяснения, по фактам, имеющим отношение к предмету разбирательства. Отказ от дачи пояснений оформляется отдельной справкой с указанием мотивов отказа;

– знакомиться с документами организации, имеющими отношение к предмету разбирательства с разрешения главой муниципального района – главой администрации Октябрьского муниципального района. В случае необходимости приобщать указанные документы либо их копии к материалам разбирательства;

– получать в установленном порядке консультации у специалистов государственной и негосударственной форм собственности по вопросам, требующим специальных познаний;

– осматривать предметы, документы, изделия, имеющие отношение к событию;

– применять для фиксации полученной информации средства аудио-, видеозаписи по правилам уголовно-процессуального законодательства, в случае возникновения такой необходимости;

– приобщать к заключению о результатах разбирательства свое особое мнение в случае несогласия с процессом разбирательства или выводами по результатам работы.

IV. Завершение разбирательства

4.1. По результатам разбирательства, проводившие его работники Администрации, составляют акт (форма акта прилагается), который представляется главе муниципального района – главе администрации Октябрьского муниципального района. В заключении должно быть указано:

– должности и фамилии работников Администрации, проводивших разбирательство и основание для его назначения;

– установочные данные лица, в отношении которого проводилось разбирательство;

– аргументированные ответы на вопросы, перечисленные в п. 3.1. настоящей инструкции;

– предложения (в зависимости от результатов разбирательства) о применении к виновному конкретного дисциплинарного взыскания, привлечения его к материальной ответственности, мерах, направленных на устранение причин и условий, способствовавших совершению проступка, о прекращении разбирательства или направлении материалов разбирательства в правоохранительные органы для решения вопроса о возбуждении уголовного дела.

4.2. Акт, подписанный работниками Администрации, проводившими разбирательство, не требует согласования с непосредственными начальниками структурных подразделений этих работников.

4.3. Глава муниципального района – глава администрации Октябрьского муниципального района, изучает собранные материалы и акт, оценивает их полноту и объективность, утверждает акт либо возвращает с конкретными указаниями о собирании дополнительных сведений. Разбирательство считается законченным в день утверждения акта. Если в ходе разбирательства будут установлены признаки состава преступления, глава муниципального района – глава администрации Октябрьского муниципального района принимает решение о направлении материалов в установленном порядке в правоохранительные органы.

4.4. Работники Администрации, в отношении которых проводилось разбирательство, должны быть ознакомлены с материалами проведенных разбирательств.

Приложение
к Инструкции о порядке проведения разбирательств
по фактам несоблюдения условий хранения
носителей персональных данных, использования
средств защиты информации в информационных
системах персональных данных в Администрации
Октябрьского муниципального района

УТВЕРЖДАЮ:
Глава муниципального района – глава администрации Октябрьского муниципального района Пермского края

_____
«____»_____20___г.

АКТ
о проведении разбирательства
по факту несоблюдения условий хранения носителей персональных данных
(использования средств защиты информации)

Комиссия в составе:
Председатель: (ФИО, должность)
Члены комиссии: (ФИО, должность)
(ФИО, должность)
(ФИО, должность)
на основании распоряжения №_____ от «__» _____ 20__ года «_____»

провела разбирательство по факту несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных и другим нарушениям, приводящим к снижению уровня защищенности персональных данных, установленного в
_____(на
именование структурного подразделения)

_____
(наименование распорядительного документа, регламентирующего указанный порядок)

Поводом для назначения разбирательства стали, поступившие сведения
_____
_____
(несоблюдения условий хранения носителей персональных данных, использования средств защиты информации в Администрации Октябрьского муниципального района)

Проведенным разбирательством установлено
_____
_____
(приводятся фактические данные, свидетельствующие об инциденте. Описываются время, место, способ и другие обстоятельства инцидента. Приводятся данные, свидетельствующие о наличии либо отсутствии вины лица. Излагаются мотив и цель нарушения (правонарушения). Указываются обстоятельства, способствовавшие инциденту).

Изложенное позволяет прийти к следующим выводам:

_____

_____

(излагаются: а) правовая оценка события; б) оценка тяжести наступивших последствий; в) правовая оценка действия лиц; г) правовая оценка действий лица, ответственного за обеспечение безопасности персональных данных и конфиденциальной информации в Администрации Октябрьского муниципального района).

По итогам разбирательства полагаем целесообразным:

_____

_____

(высказывается мнение комиссии о наличии (отсутствии) признаков преступления в действиях конкретного лица, по вине которого произошел инцидент. О целесообразности передачи собранных материалов в органы следствия (суд). При установлении нарушения установленного порядка хранения носителей персональных данных или использования средств защиты, способствовавшего нарушению конфиденциальности персональных данных, высказывается мнение о целесообразности наказания виновного в рамках трудового или иного законодательства).

Председатель комиссии _____
(подпись)

Члены комиссии _____
(подписи)

УТВЕРЖДЕНА:
постановлением Администрации Октябрьского муниципального района Пермского края
от 02.03.2018 № 118-266-01-05

ИНСТРУКЦИЯ
работников Администрации Октябрьского муниципального района, допущенных к обработке конфиденциальной информации и персональных данных

I. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012г. №1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Данная инструкция определяет общие обязанности, права и ответственность пользователя информационных систем Администрации Октябрьского муниципального района по обеспечению информационной безопасности при работе со сведениями конфиденциального характера и персональных данных.

1.3. Пользователем информационной системы (далее – Пользователь) является работник Администрации Октябрьского муниципального района, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до работников Администрации под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

II. Обязанности пользователя

2.1. При выполнении работ в ИС Пользователь обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, правила работы и порядок регистрации в ИС, доступа к информационным ресурсам ИС;

– знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее - АРМ);

– хранить втайне свои идентификационные данные (имена, пароли и т. д.);

– выполнять требования, предъявляемые к парольной системе (нормативы на длину, состав, периодичность смены пароля и т. д.), осуществлять вход на АРМ только под своими идентификационными данными;

– выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей ИС;

– немедленно вызывать работника сектора информационного и технического обеспечения Администрации района и ставить в известность руководителя своего подразделения в случае утери индивидуального устройства идентификации (ЭЦП- электронно-цифровая подпись) или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии

номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной АРМ, несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;

– присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ, ставить в известность работника сектора информационного и технического обеспечения Администрации района при необходимости внесения изменения в состав аппаратных и программных средств АРМ;

– работать в ИС только в разрешенный период времени;

– немедленно выполнять предписания и предоставлять свое АРМ работникам сектора информационного и технического обеспечения Администрации района для контроля;

– ставить в известность работников сектора информационного и технического обеспечения Администрации района в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т. п.), а также перебоев в системе электроснабжения;

– осуществлять уничтожение информации, содержащей сведения о конфиденциальной информации и персональных данных, с машинных носителей информации и из оперативной памяти АРМ;

– уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;

– сообщать руководителю своего подразделения обо всех проблемах, связанных с эксплуатацией ИС.

2.2. Пользователю категорически запрещается:

– использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

– самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИС (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формуляром АРМ;

– осуществлять обработку информации, содержащей сведения конфиденциального характера и персональные данные, в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить конфиденциальную информацию и персональные данные на неучтенных носителях информации, в том числе для временного хранения;

– оставлять включенное без присмотра АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);

– передавать кому-либо свое индивидуальное устройство идентификации (ЭЦП) в нарушение установленного порядка, делать неучтенные копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;

– оставлять без личного присмотра на рабочем месте или где бы то ни было свою ЭЦП, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (конфиденциальную информацию и персональные данные);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИС (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность работников сектора информационного и технического обеспечения Администрации района и руководителя своего подразделения;

– подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;

– осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;

– фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;

– разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера и персональные данные;

– вносить изменения в файлы, принадлежащие другим пользователям.

III. Права пользователя

3.1. Пользователь имеет право:

– присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;

– участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;

– своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;

– требовать от администратора безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

IV. Правила работы в сетях общего доступа

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИС, должна производиться при служебной необходимости.

4.2. При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирусной защиты, средств от несанкционированного доступа и т. д.);

– передавать по Сети защищаемую информацию без использования средств защиты каналов связи;

– запрещается загружать из Сети программное обеспечение;

– запрещается посещение сайтов сомнительной репутации (аморального содержания, содержащие нелегально распространяемое программное обеспечение или иной контент);

– запрещается нецелевое использование подключения к сети.

V. Ответственность пользователя

5.1. Пользователь несет персональную ответственность за:

– ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, индивидуального средства идентификации и целостность установленного программного обеспечения.

– разглашение сведений, отнесенных к сведениям конфиденциального характера и персональным данным, и сведений ограниченного распространения, ставших известными ему по роду работы.

5.2. Ответственность за нарушение функционирования ИС, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими

идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного разбирательства.

5.3. Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации.

5.4. Разглашение персональных данных (ПДн) субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих ПДн субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно - правовыми актами Администрации Октябрьского муниципального района, влечет наложение на сотрудника, имеющего доступ к ПДн, дисциплинарных взысканий в соответствии со ст. 192 ТК РФ «Дисциплинарные взыскания». Работник Администрации, имеющий доступ к персональным данным субъекта и совершивший дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Администрации (в соответствии с п. 7 ст. 243 ТК РФ «Случаи полной материальной ответственности»).

5.5. В отдельных случаях, при разглашении конфиденциальной информации и персональных данных, работник, совершивший проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ «Разглашение информации с ограниченным доступом».

5.6. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушение неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 УК РФ «Нарушение неприкосновенности частной жизни».

УТВЕРЖДЕНА:
постановлением Администрации Октябрьского муниципального района Пермского края
от 02.03.2018 № 118-266-01-05

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах Администрации Октябрьского муниципального района Пермского края

I. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных».

1.2. Данная инструкция определяет порядок действий пользователя при возникновении нештатной ситуации при работе с персональными данными в информационной системе персональных данных (далее – ИС) Администрации Октябрьского муниципального района Пермского края (далее - Администрация района) и по реагированию на нештатные ситуации, связанные с работой в ИС.

1.3. Пользователем ИС (далее – Пользователь) является сотрудник Администрации района, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС согласно списка лиц, которым необходим доступ к персональным данным, обрабатываемым в ИС, для выполнения своих должностных обязанностей.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

II. Общий порядок действий при возникновении нештатных ситуаций

2.1. В настоящем документе под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС, а так же с вероятностью потери защищаемой информации.

2.2. К нештатным ситуациям относятся следующие ситуации:

– сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, ошибки в работе программы и т. п.);

– отключение электричества;

– сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);

– выход из строя сервера;

– потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие

связи с сервером, повреждение файлов и т. п.);

– обнаружен вирус;

– обнаружена утечка информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);

– взлом системы (web-сервера, файл-сервера и др.) или несанкционированный доступ;

– попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);

– компрометация ключей (утеря носителя ключевой информации (Rutoken, E-token и т. п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место, взлом учётной записи пользователя);

– компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);

– физическое повреждение ЛВС или ПЭВМ (не включается ПК, при попытке включения отображается синий или черный экраны, повреждены провода и т. п.);

– стихийное бедствие;

– иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИС и возможность потери защищаемой информации, и названные таковыми пользователем ИС или администратором безопасности ИС.

2.3. При возникновении нештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность администратора безопасности. В случае, если поставить в известность администратора не представляется возможным (администратор безопасности отсутствует на рабочем месте), пользователем, обнаружившим нештатную ситуацию, составляется служебная записка в свободной форме с описанием нештатной ситуации, и передается руководителю подразделения.

2.4. Администратор безопасности ИСПДн проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего непосредственного начальника для определения дальнейших действий. Здесь и далее – в случае отсутствия администратора безопасности, все действия и меры в отношении нештатной ситуации, описанные в настоящей инструкции, выполняет другой сотрудник структурного подразделения Администрации района, отвечающие за деятельность информационного и технического обеспечения деятельности Администрации района.

2.5. По факту возникновения и устранения нештатной ситуации заносится запись в «Журнал учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах ИС Администрации района».

2.6. При необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

III. Особенности действий при возникновении наиболее распространенных нештатных ситуаций

3.1. **Сбой программного обеспечения.** Администратор безопасности ИСПДн совместно с сотрудником структурного подразделения Администрации района, у которого произошла нештатная ситуация, выясняют причину сбоя. Если исправить ошибку своими силами не удалось, разработчику ПО направляется информационное сообщение с сопроводительными материалами о возникшей ситуации.

3.2. **Отключение электричества.** Администратор безопасности ИСПДн совместно с

сотрудником структурного подразделения Администрации района, у которого произошла нештатная ситуация, проводят анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

3.3. **Сбой в локальной вычислительной сети (ЛВС).** Администратор безопасности ИСПДн проводит анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

3.4. **Выход из строя сервера.** Администратор безопасности ИСПДн, ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера (если есть) для обеспечения непрерывной работы Администрации района. При необходимости производятся работы по восстановлению ПО и данных из резервных копий.

3.5. **Потеря данных.** При обнаружении потери данных Администратор безопасности ИСПДн проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий.

3.6. **Обнаружен вирус.** При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится компетентным в этой области сотрудником. Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться «Инструкцией по организации антивирусной защиты», инструкцией по эксплуатации применяемого антивирусного ПО. После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ЭВМ Администрации района с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий. Проводится служебное расследование по факту появления вируса в ЭВМ (ЛВС).

3.7. **Обнаружена утечка информации.** При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

3.8. **Взлом системы (Web-сервера, файл-сервера и др.) или несанкционированный доступ (НСД).** При обнаружении взлома сервера ставится в известность Администратор безопасности ИСПДн. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянских закладок. Возможен временный переход на резервный сервер. Учитывая, что программные закладки могут быть не обнаружены антивирусным ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС Администрации района, после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ. По факту взлома сервера проводится служебное расследование.

3.9. **Попытка несанкционированного доступа (НСД).** При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн. При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД (данный журнал ведется автоматизированным способом средствами защиты информации от несанкционированного доступа). По результатам анализа, в случае

необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

3.10. **Компрометация ключей.** При обнаружении утечки информации ставится в известность Администратор безопасности и начальник подразделения. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

3.11. **Компрометация пароля.** При обнаружении утечки информации ставится в известность Администратор безопасности и ответственное лицо Администрации района за ООиЗПД. При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т.д.). При необходимости, проводится служебное расследование.

3.12. **Физическое повреждение ЛВС или ПЭВМ.** Ставится в известность Администратор безопасности ИСПДн. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

3.13. **Стихийное бедствие.** При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими поведение в чрезвычайных ситуациях, принятых в учреждении.

IV. Меры против возникновения нештатных ситуаций

4.1. Администратором безопасности ИСПДн периодически, не реже 1 раза в год, должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

4.2. В общем случае, для предотвращения нештатных ситуаций необходимо четкое соблюдение требований нормативных документов и инструкций по эксплуатации оборудования и ПО.

4.3. Рекомендации по предотвращению некоторых типичных нештатных ситуаций:

– Сбой программного обеспечения -применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на ЭВМ (проверка диска и др.).

– Отключение электричества - использовать источники бесперебойного питания на критически важных технологических участках Администрации района.

– Сбой ЛВС - обеспечение бесперебойной работы ЛВС путем применения надежных сетевых технологий и резервных систем.

– Выход из строя серверов - применять надежные программно-технические средства. Допускать к работе с серверным оборудованием только квалифицированных специалистов.

– Потеря данных - периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации. Проводить с администраторами информационной безопасности (и сотрудниками) разъяснительные и обучающие собрания. Обеспечить резервное копирование данных.

– Обнаружение вируса - соблюдать требования «Инструкции по организации антивирусной защиты».

– Утечка информации -применять средства защиты от НСД. Регулярно проводить анализ журналов попыток НСД и работы по совершенствованию системы защиты информации.

– Попытка несанкционированного доступа (НСД) - по возможности, установить регистрацию попыток НСД на всех технологических участках, где возможен

несанкционированный доступ, с оповещением Администратора информационной безопасности о попытках НСД.

– Компрометация паролей - соблюдать требования «Инструкции по организации парольной защиты».

– Физическое повреждение ЛВС или ПЭВМ - физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним.

– Стихийное бедствие - проводить обучающие собрания и тренировки персонала Администрации района по вопросам гражданской обороны.

УТВЕРЖДАЮ:
Глава муниципального района – глава администрации Октябрьского муниципального района Пермского края
_____Г.В. Поезжаев
«____»_____20___г.

Журнал
по учету обращений субъектов персональных данных о выполнении их законных прав в области обработки и защиты персональных данных, в том числе в информационных системах персональных данных

Журнал начат «__»_____ 201__г.
Журнал завершен «__» _____ 201__г.

ОТВЕТСТВЕННЫЙ
за ведение журнала
_____
_____ _____
«___» _____ 201__г.

№ п/п	Дата обращения	ФИО субъекта ПДн (запрашивающее лицо)	Краткое содержание обращения	Цель получения запрашиваемых ПДн
1	2	3	4	5

Отметка о предоставлении информации или отказе в её предоставлении	Дата передачи или отказа в предоставлении информации	Подпись запрашивающего лица	Подпись ответственного лица	Примечание
6	7	8	9	10

УТВЕРЖДАЮ:
Глава муниципального района – глава администрации Октябрьского муниципального района Пермского края
_____Г.В. Поезжаев
«____»_____20___г.

Журнал
учета проверок юридического лица, проводимых органами государственного контроля (надзора), органами муниципального контроля

_____
(дата начала ведения Журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____

_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала учета проверок)

_____

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____
М.П.

1	Дата начала и окончания проверки	
2	Общее время проведения проверки (в отношении субъектов малого предпринимательства и микро-предприятий указывается в часах)	
3	Наименование органа государственного контроля (надзора), наименование органа муниципального контроля	
4	Дата и номер распоряжения или приказа о проведении проверки	
5	Цель, задачи и предмет проверки	
6	Вид проверки (плановая или внеплановая): в отношении плановой проверки: – со ссылкой на ежегодный план проведения проверок; в отношении внеплановой выездной проверки: – с указанием на дату и номер решения прокурора о согласовании проведения проверки (в случае, если такое согласование необходимо)	
7	Дата и номер акта, составленного по результатам проверки, дата его вручения представителю юридического лица, индивидуальному предпринимателю	
8	Выявленные нарушения обязательных требований (указываются содержание выявленного нарушения со ссылкой на положение нормативного правового акта, которым установлено нарушенное требование, допустившее его лицо)	
9	Дата, номер и содержание выданного предписания об устранении выявленных нарушений	
10	Фамилия, имя, отчество (в случае, если имеется), должность должностного лица (должностных лиц), проводящего(их) проверку	
11	Фамилия, имя, отчество (в случае, если имеется), должности экспертов, представителей экспертных организаций, привлеченных к проведению проверки	
12	Подпись должностного лица (лиц), проводившего проверку	

УТВЕРЖДАЮ:
Глава муниципального района – глава администрации Октябрьского муниципального района Пермского края
_____Г.В. Поезжаев
«____»_____20___г.

ЖУРНАЛ
ПРОВЕДЕНИЯ ИНСТРУКТАЖА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Журнал начат «__»_____ 201__г.
Журнал завершен «__» _____ 201__г.

ОТВЕТСТВЕННЫЙ
за ведение журнала
_____
_____
«___» _____ 201__г.

№	ФИО	Дата	Должность	Подразде-ление	Подпись об ознакомлении с локальными нормативными актами
1	2	3	4	5	6