**Министерство социальной политики и труда Удмуртской Республики**
(Минсоцполитики УР)

**Удмурт Элькунысь мерлыко политикая но ужъя министерство**
(УЭ мерполитикмин)

# ПРИКАЗ

«14» июня 2019 г. № 166

г. Ижевск

**Об утверждении Инструкции пользователя информационных систем по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Министерстве социальной политики и труда Удмуртской Республики**

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» п р и к а з ы в а ю:

1. Утвердить прилагаемую Инструкцию пользователя информационных систем по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Министерстве социальной политики и труда Удмуртской Республики.

2. Признать утратившим силу приказ Министерства социальной, семейной и демографической политики Удмуртской Республики от 30 декабря 2015 года № 349 «Об утверждении Инструкции пользователя информационных систем по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Министерстве социальной, семейной и демографической политики Удмуртской Республики».

Министр Т.Ю. Чуракова

УТВЕРЖДЕНА

приказом Министерства
социальной политики и труда
Удмуртской Республики
от «14» июня 2019 года № 166

# ИНСТРУКЦИЯ
## пользователя информационных систем по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Министерстве социальной политики и труда Удмуртской Республики

### I. Общие положения

1. Настоящая Инструкция определяет возможные внештатные ситуации, связанные с функционированием информационных систем Министерства социальной политики и труда Удмуртской Республики (далее соответственно – информационные системы, Министерство), порядок действий сотрудников Министерства, осуществляющих обработку персональных данных в информационных системах, принимаемые меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем.

2. Пользователем информационных систем по обеспечению безопасности обработки персональных данных является сотрудник Министерства, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, персональным данным и средствам защиты информации (далее – пользователь).

3. Пользователь несёт персональную ответственность за свои действия.

### II. Порядок реагирования на внештатную ситуацию

4. Под внештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов информационной системы, а так же с вероятностью потери защищаемой информации.

5. Критичность внештатной ситуации оценивается администратором безопасности, администратором информационной системы и пользователем (далее – специалисты, ответственные за реагирование) на основе следующей классификации:

уровень 1 – незначительный инцидент (локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов информационной системы и средств защиты информации);

уровень 2 – авария (инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов информационной системы и средств защиты информации);

уровень 3 – катастрофа (инцидент, приводящий к полному прерыванию работоспособности всех элементов информационных систем и средств защиты информации более чем на сутки, а также к угрозе жизни пользователей).

6. К внештатным ситуациям относятся следующие ситуации:

сбой в работе программного обеспечения;

потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т. п.);

обнаружение компьютерного вируса;

выход из строя сервера;

обнаружение утечки информации (взлом учётной записи пользователя, обнаружение посторонних устройств в системном блоке и т. п.);

взлом системы (web-сервера, файл-сервера и др.);

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 учётной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);

физическое повреждение компьютера;

сбой в локальной вычислительной сети;

отказ элементов информационной системы и средств защиты информации из-за отключения электроэнергии, повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), стихийного бедствия (пожар в здании Министерства, взрыв, просадка грунта с частичным обрушением здания Министерства, массовые беспорядки в непосредственной близости от здания Министерства и т. п.);

иные внештатные ситуации, влекущие за собой повреждение элементов информационной системы и возможность потери защищаемой информации.

7. При возникновении внештатной ситуации 1 уровня инцидент решается специалистами, ответственными за реагирование, в следующем порядке:

пользователь, обнаруживший внештатную ситуацию, немедленно ставит в известность администратора безопасности и руководителя структурного подразделения Министерства;

администратор безопасности проводит предварительный анализ внештатной ситуации на наличие потерь и (или) разрушений баз данных и программного обеспечения, проверяет работоспособность оборудования;

совместно с пользователем, у которого произошла внештатная ситуация, администратор безопасности выясняет причину сбоя в работе информационной системы и возможные угрозы безопасности информации;

в кратчайшие сроки, не превышающие одного рабочего дня, специалисты, ответственные за реагирование, принимают меры по восстановлению работоспособности информационной системы; в случае необходимости, производят восстановление баз данных и программного обеспечения из резервных копий;

по факту возникновения и устранения внештатной ситуации заносится запись в журнал по учёту мероприятий по контролю обеспечения защиты персональных данных в информационных системах Министерства;

при необходимости, проводится служебное расследование по факту возникновения внештатной ситуации и выяснению её причин.

8. При возникновении внештатной ситуации 2 или 3 уровня инцидент выходит за рамки управления специалистами, ответственными за реагирование и должен быть незамедлительно доложен должностному лицу, ответственному за защиту информации в Министерстве. Специалисты, ответственные за реагирование, в этом случае руководствуются документами, регламентирующими поведение в чрезвычайных ситуациях.

## III. Меры обеспечения непрерывности работы и восстановления информационных систем при возникновении внештатных ситуаций

9. К техническим мерам обеспечения непрерывной работы и восстановления информационных систем относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

10. Системы жизнеобеспечения информационных систем включают в себя:

пожарную сигнализацию и систему пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

11. Все помещения Министерства, в которых размещаются элементы информационных систем и средства защиты информации, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

12. К организационным мерам обеспечения непрерывной работы и восстановления информационных систем относятся:

ознакомление пользователей с локальными документами Министерства в области защиты информации, в том числе с Инструкцией пользователя информационных систем персональных данных Министерства социальной

политики и труда Удмуртской Республики, утверждённой приказом Министерства от 14 февраля 2018 года № 85, и настоящей Инструкцией;

обучение пользователей порядку действий при возникновении внештатных ситуаций;

проверка навыков и знаний администратора безопасности и администратора информационной системы о порядке реагирования на возникновение внештатных ситуаций;

проведение администратором безопасности ежегодного анализа зарегистрированных внештатных ситуаций для выработки мероприятий по их предотвращению.