ОТДЕЛ ОБРАЗОВАНИЯ
АДМИНИСТРАЦИИ ВАРГАШИНСКОГО РАЙОНА

ПРИКАЗ

от 10.04.2017г. **№** 35
р.п. Варгаши

Об утверждении инструкции по обеспечению безопасности персональных данных при возникновении внештатных ситуаций в Отделе образования Администрации Варгашинского района

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказомФедеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по обеспечению безопасности персональных данных при возникновении внештатных ситуаций в Отделе образования Администрации Варгашинского района, согласно приложению к настоящему приказу.

2. Контроль за выполнением настоящего приказа возложить на начальника службы организационно-правовой и кадровой работы Отдела образования Администрации Варгашинского района Радковскую Л.Н.

Начальник Отдела образования
Администрации Варгашинского района Копия С.А. Кожева

Приложение к приказу
Отдела образования Администрации
Варгашинского района
от _____ № _____
«Об утверждении инструкции по обеспечению
безопасности персональных данных
при возникновении внештатных ситуаций
в Отделе образования Администрации
Варгашинского района»

Инструкция
по обеспечению безопасности персональных данных
при возникновении внештатных ситуаций
в Отделе образования Администрации Варгашинского района

I. Общие положения

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных системах персональных данных (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций в Отдела образования Администрации Варгашинского района (далее – Отдел образования).

2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

3. Действие настоящей Инструкции распространяется на всех пользователей Отдела образования, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций в том числе:

- системы жизнеобеспечения;
-системы обеспечения отказоустойчивости;
-системы резервного копирования и хранения данных;
-системы контроля физического доступа.

II. Порядок реагирования на аварийную ситуацию

4. Действия при возникновении аварийной ситуации.

В настоящей инструкции под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится

возможной в результате реализации одной из угроз, согласно Приложению к данной инструкции.
Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование пользователем в «Журнале ИСПДн».

В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности на объектах информатизации, начальники отделов и пользователи ИСПДн Отдела образования предпринимают меры по восстановлению работоспособности ИСПДн. Принимаемые меры согласуются с начальником Отдела образования.

5. Уровни реагирования на инцидент.

При реагировании на инцидент, важно, чтобы пользователь ИСПДн правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

уровень 1 – незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

уровень 2 – авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

1) отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования;

2) отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

- химического выброса в атмосферу;
- сбоев общественного транспорта;
- эпидемии;
- массового отравления персонала;
- сильного снегопада;
- сильных морозов.

уровень 3 – катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа.
К катастрофам относятся следующие инциденты:

1) пожар в здании;
2) взрыв;
3) просадка грунта с частичным обрушением здания;

4) массовые беспорядки в непосредственной близости от Объекта.

III. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

6. Технические меры.

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

1) системы жизнеобеспечения;
2) системы обеспечения отказоустойчивости;
3) системы резервного копирования и хранения данных;

Системы жизнеобеспечения ИСПДн включают:

1) пожарные сигнализации и системы пожаротушения;
2) системы резервного питания.

Все критичные помещения Отдела образования (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Регламенте проведения резервного копирования (восстановления)технических систем и программного обеспечения, баз данных и средств защиты информации, хранящиеся на автоматизированных рабочих местах и серверах Отдела образования Администрации Варгашинского района, утвержденным приказом № _____ от _____ 20___ года.

7. Организационные меры.

Администратор безопасности Отдела образования ознакамливает всех сотрудников Отдела образования, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в журнале, предоставляемом Администратором безопасности. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Приложение
к инструкции по обеспечению
безопасности персональных данных
при возникновении внештатных
ситуаций в Отделе образования
Администрации Варгашинского
района

Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телеком и ИТ угрозы	
17	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	

18	Ошибка персонала, имеющего доступ к серверной
19	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
20	Отключение электроэнергии
21	Сбой в работе интернет-провайдера
22	Физически разрыв внешних каналов связи