УТВЕРЖДАЮ
Директор школы _____ И.В. Абрамова
Приказ № 104 от 30.12. 2020 г.

ИНСТРУКЦИЯ
по устранению причин и последствий инцидентов

1. Введение.

1.1. Настоящая инструкция предназначена для обеспечения защиты информации, содержащейся в автоматизированной информационной системе МБОУСОШ № 8 (далее – АИС), в том числе персональных данных (далее – ПДн), с помощью устранения причин и последствий инцидентов.

1.2. Настоящая инструкция определяет порядок действий **администратора безопасности** и администраторов системных АИС при устранении причин и последствий инцидентов безопасности в АИС.

2. Обеспечение возможности устранения последствий инцидентов.

2.1. Обеспечение возможности устранения последствий инцидентов осуществляется резервным копированием информации, обрабатываемой в АИС на съемные машинные носители **не реже, чем раз в неделю**, и организацией их учета и защищенного хранения.

2.2. Сведения о проведении процедуры резервного копирования администратор безопасности заносит в **журнал учета резервного копирования**.

2.3. Машинные носители, на которые произведено резервное копирование, должны быть пронумерованы: **номером носителя и датой проведения резервного копирования**. Хранение и доступ к носителям в соответствии с требованиями «Инструкции по защите машинных носителей информации». Носители должны храниться не менее года, для возможности восстановления данных.

3. Порядок устранения последствий инцидента

3.1. Ответственным лицом за устранение последствий инцидента в Организации является **администратор безопасности**. При устранении последствий инцидента администратор безопасности вправе привлекать к работам по устранению инцидента администраторов системных АИС.

3.2. **Администратор безопасности** приступает к устранению последствий инцидента немедленно после распоряжения **ответственного за защиту информации**.

3.3. При нарушении конфиденциальности информации, обрабатываемой в АИС или подозрении в ее нарушении администратор безопасности:

3.3.1. проводит процедуру смены паролей пользователям;

3.3.2. пересматривает и обновляет, с учетом содержания инцидента, матрицу доступа к информации, обрабатываемой в АИС.

3.4. При нарушении целостности и доступности информации администратор безопасности:

3.4.1. организует переустановку программного обеспечения АИС и системы защиты информации с эталонных копий используемого ПО;

3.4.2. организует переустановку обрабатываемой информации, в том числе персональные данные, с резервных копий;

3.4.3. проверяет конфигурацию АИС и ее системы защиты информации (при необходимости восстанавливает конфигурацию в соответствии с эксплуатационной документацией);

3.4.4. осуществляет действия по п. 3.3. (при подозрении на умышленное нарушение целостности и доступности).

3.5. Результаты устранения последствий инцидента оформляются Актом устранения последствий инцидента.

4. Порядок устранения причин инцидента

4.1. Причины инцидента устанавливаются при анализе инцидента, который организует **ответственный за защиту информации**.

4.2. Причины инцидентов в АИС разделяют на типы:

4.2.1. аппаратно-программные причины;

4.2.2. организационные причины.

4.3. К аппаратно-программным причинам относятся все причины, связанные с недостатками аппаратной и программной частей АИС и ее системы защиты информации (ошибки кода, ошибки настроек, неисправности оборудования, электромагнитная совместимость и т.п.).

4.4. К организационным причинам относятся недостатки организационно-распорядительной документации, ошибки пользователей, недостатки физической защиты доступа, дисциплинарные, злой умысел и т.п.

4.5. Устранение аппаратно-программных причин инцидентов осуществляет **администратор безопасности**. Сроки и состав действий определяются индивидуально по каждому инциденту, утверждаются и контролируются **ответственным за защиту информации.**

4.6. Устранение организационных причин осуществляет **ответственный за защиту информации**. Сроки и состав действий определяются индивидуально ответственным за защиту информации по каждому инциденту.

4.7. Результаты устранения причин инцидентов оформляются **Актом устранения причин инцидента.**

5. Заключительные положения.

5.1. Администратор безопасности и администраторы системные АИС должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.

5.2. Администратор безопасности и администраторы системные АИС должны быть ознакомлены с настоящей инструкцией до начала работы с АИС под роспись. Обязанность ознакомления администратора безопасности и администраторов системных АИС с настоящей инструкцией лежит на **ответственном за защиту информации.**

6. Нормативные и правовые документы.

1.1. Методический документ, утвержден ФСТЭК России 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Приказ ФСТЭК России от 18.02.2013 года **№21** «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Постановление Правительства РФ от 01.11.2012 **№1119** «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.4. Постановление правительства РФ от 21.03.2012 **№211** «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».