Утверждаю: директор
МБОУ СШ №66
_____О.В. Мединская
Приказ № 01-10-262
От 24.09.2020 г

ИНСТРУКЦИЯ
администратора безопасности информации в МБОУ СШ № 66

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности должностного лица, ответственного за обеспечение безопасности информации в МБОУ СШ № 66 (далее — администратор безопасности информации), в том числе персональных данных (далее ПДн), обрабатываемой в информационных системах ПДн (далее — ИСПДн) в МБОУ СШ № 66 (далее — Учреждение).

1.2. Действие настоящей Инструкции распространяется на структурные подразделения Учреждения.

1.3. Администратор безопасности информации назначается приказом директора школы.

1.4. Администратор безопасности информации по вопросам обеспечения безопасности информации подчиняется директору школы.

1.5. Администратор безопасности информации отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн.

1.6. Администратор безопасности информации осуществляет методическое руководство деятельностью пользователей ИСПДн Учреждения по вопросам обеспечения безопасности информации.

1.7. Требования администратора безопасности информации, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн Учреждения.

.8. Администратор безопасности информации несёт персональную ответственность за качество проводимых им работ по контролю действий должностных лиц МБОУ СШ № 66 (далее пользователи) при работе в ИСПДн Учреждения, состояние и поддержание установленного уровня защищенности информации, обрабатываемой в ИСПДн Учреждения.

2. Задачи администратора безопасности информации

2.1. Основными задачами администратора безопасности информации являются:

- поддержание необходимого уровня защищенности ИСПДн Учреждения от несанкционированного доступа (далее — НСД) к информации;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;
- установка средств защиты информации и контроль выполнения правил их эксплуатации;
- сопровождение средств защиты информации (далее — СЗИ) от НСД *н основных* технических средств и систем *[Далее* — ОТСС) ИСПДн *Учреждения,-*

- периодическое обновление СЗИ и проведение комплекса мероприятий по предотвращению нарушений требований информационной безопасности (далее — ИБ);

- оперативное реагирование на нарушения требований по ИБ в ИСПДн Учреждения и участие в их предотвращении (нейтрализации).

2.2. В рамках выполнения основных задач администратор безопасности информации осуществляет:

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

- текущий контроль технологического процесса автоматизированной обработки

- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;

- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в структурных подразделениях Учреждения;

- методическую помощь пользователям ИСПДн Учреждения по вопросам обеспечения безопасности ПДн.

3. Обязанности администратора безопасности информации

Администратор безопасности информации обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн Учреждения.

3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.

3.3. Участвовать в приемке новых программных средств обработки информации.

3.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн Учреждения согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн Учреждения при обработке ПДн.

3.6. Вести контроль осуществления резервного копирования информации.

3.7. Анализировать состояние затиты ИСПДн Учреждения.

3.8. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.9. Контролировать физическую сохранность технических средств обработки информации.

3.10. Контролировать исполнение пользователями ИСПДн Учреждения введенного режима безопасности. а также правильность работы с элементами ИСПДн Учреждения и средствами защиты информации.

3.11. Контролировать исполнение пользователями ИСПДн Учреждения правил парольной политики.

3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей ИСПДн Учреждения и вы явления возможных нарушений.

3.13. Не допускать установку, использование, хранение и размнокение в ИСПДн Учреждения программных средств, не связанных с выполнением функциональных задач.

3.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест ИСПДн Учреждения.

3.15. Оказывать помощь пользователям ИСПДн Учреждения в части применения

СЗИ и консультировать по вопросам введенного режима защиты.

3.16. Периодически представлять руководству отчет о состоянии СЗИ ИСПДн Учреждения, о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн Учреждения, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.18. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.19. Принимать участие в проведении работ по оценке соответствия ИСПДн Учреждения требованиям безопасности информации.

4. Права администратора безопасности информации

Администратор безопасности информации имеет право:

4.1. Отключать от ресурсов ИСПДн Учреждения пользователей, осуществивших НСД к защищаемым ресурсам ИСПДн Учреждения или нарушивших другие требования по ИБ.

4.2. Давать сотрудникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, несанкционированного доступа, утраты, порчи защищаемой информации и технических средств ИСПДн Учреждения.

4.4. Организовывать и участвовать в любых проверках по использованию пользователями Учреждения телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн Учреждения при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с руководством и персоналом Учреждения по вопросам обеспечения ИБ.

4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.8. Запрашивать и получать от пользователей ИСПДн Учреждения информацию и материалы, необходимые для организации своей работы.

4.9. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ ПДн, обрабатываемых в Учреждении.

5. Ответственность администратора безопасности информации

Администратор безопасности несет ответственность за:

5.1. Организацию защиты информационных ресурсов и технических средств ИСПДн Учреждения.

5.2. Качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защищенности информационных и технических ресурсов ИСПДн Учреждения.

5.3. Разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

6. Действия администратора безопасности информации при обнаружении попыток НСД

6.1. К попыткам НСД относятся:

сеансы работы с телекоммуникационными ресурсами Учреждения незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;

действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн Учреждения с использованием учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

6.2. При выявлении факта (попытки) НСД администратор безопасности обязан:

прекратить доступ к информационным ресурсам со стороны выявленного участка НСД:

доложить директору школы о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

известить директора школы, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

проанализировать характер НСД;

по решению директора школы осуществить действия по выяснению причин, приведших к НСД;

предпринять меры по предотвращению подобных инцидентов в дальнейшем.