Приложение № 6
к приказу МОУ СОШ № 50
г. Комсомольска-на-Амуре
от 27.08.2015 г. № 265

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных информационных систем персональных данных в МОУ СОШ №50 города Комсомольска-на-Амуре

I. Общие положения

1. Настоящая инструкция (далее – Инструкция) определяет общие функции, ответственность, права и обязанности ответственного за обеспечение безопасности персональных данных информационных систем персональных данных (далее – Ответственный) в Муниципальном общеобразовательном учреждении средняя общеобразовательная школа №50г.Комсомольска-на-Амуре (далее «Учреждение»).

2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

3. Ответственный назначается приказом по «Учреждению» на основании «Положения о разграничении прав доступа к обрабатываемым персональным данным» в «Учреждении» из числа штатных сотрудников.

4. Ответственный подчиняется непосредственно Директору «Учреждения».

5. На время отсутствия Ответственного (отпуск, болезнь, пр.) его обязанности исполняет лицо, назначенное в установленном порядке, которое приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

6. Ответственный в своей работе руководствуется настоящей Инструкцией, Политикой информационной безопасности «Учреждения», другими регламентирующими документами «Учреждения», руководящими и нормативными документами регуляторов Российской Федерации в области обеспечения безопасности персональных данных.

7. Методическое руководство работой Ответственного осуществляется ответственным за организацию обработки персональных данных в «Учреждении».

8. Ответственный является ответственным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию необходимого уровня защищенности ИСПДн «Учреждения» и их ресурсов на этапах эксплуатации и модернизации.

II. Организация работы

1. Ответственный должен иметь специальное рабочее место, размещённое на территории контролируемой зоны, установленной приказом директора «Учреждения», чтобы исключить несанкционированный доступ к нему посторонних лиц и других сотрудников «Учреждения».

2. Рабочее место Ответственного должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а так же средствами контроля технических средств защиты информации (далее – СЗИ).

III. Обязанности

Ответственный должен:

1. Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов «Учреждения» в области обработки и защиты персональных данных.

2. Поддерживать необходимый уровень защищенности (режим безопасности) персональных данных при их обработке в ИСПДн согласно «Инструкции по обеспечению безопасности персональных данных».

3. Наделять и изменять права доступа всех групп пользователей ИСПДн к персональным данным и защищаемым программным ресурсам и портам ввода-вывода ИСПДн.

4. Осуществлять установку, настройку и сопровождение программных и технических СЗИ.

5. Осуществлять методическое руководство всех групп пользователей «Учреждения» в вопросах функционирования СЗИ и введенного режима защиты.

6. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

7. Участвовать в приемке новых программных и технических средств, в том числе СЗИ.

8. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений «Правил обработки персональных данных».

9. Обеспечить доступ к защищаемой информации всем группам пользователей ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

10. Уточнять в установленном порядке обязанности всех групп пользователей ИСПДн по обеспечению безопасности персональных данных.

11. Вести контроль над процессом осуществления резервного копирования баз данных и настроек комплекса средств автоматизации ИСПДн согласно «Инструкции по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и СЗИ».

12. Осуществлять контроль порядка учёта, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

13. Осуществлять контроль выполнения Плана мероприятий по обеспечению защиты персональных данных в «Учреждении».

14. Анализировать состояние защиты ИСПДн и их отдельных подсистем.

15. Контролировать неизменность состояния СЗИ, их параметров и режимов защиты.

16. Контролировать физическую сохранность СЗИ и оборудования ИСПДн.

17. Контролировать исполнение всеми группами пользователей ИСПДн введённого режима защищенности, а так же правильность работы с элементами ИСПДн и СЗИ.

18. Контролировать исполнение всем группами пользователей ИСПДн парольной политики согласно «Инструкции по организации парольной защиты»

19. Организовывать антивирусную защиту всех элементов ИСПДн согласно «Инструкции по организации антивирусной защиты».

20. Своевременно анализировать журнал учёта событий, регистрируемых СЗИ, с целью выявления возможных нарушений.

21. Недопускать установку, использование, хранение и размножение в ИСПДн ПО, не связанных с выполнением функциональных задач.

22. Не допускать к работе на элементах ИСПДн посторонних лиц.

23. Регистрировать факты выдачи внешних носителей в «Журнале учета мобильных технических средств».

24. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.

25. Периодически представлять руководству отчёт о состоянии и о нештатных ситуациях на объектах ИСПДн и допущенных всеми группами пользователей нарушениях и установленных требований по защите информации.

26. В случае отказа работоспособности СЗИ ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

27. Принимать меры по реагированию в случае возникновения нештатных или аварийных ситуаций с целью ликвидации их последствий.

28. Предлагать руководству мероприятия по совершенствованию работы по защите персональных данных.

IV. Права

Ответственный имеет право:

1. Требовать от всех групп пользователей ИСПДн соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов «Учреждения» в области обработки и защиты персональных данных.

2. Запрещать всем группам пользователей ИСПДн доступ к персональным данным при нарушении «Правил обработки персональных данных», при неисправностях в работе СЗИ и с целью предотвращения несанкционированного доступа к охраняемой информации.

3. Участвовать в анализе ситуаций, касающихся функционирования СЗИ, и в расследованиях по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.

4. Вносить предложения руководству по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

5. В пределах своей компетенции сообщать руководству о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить предложения по их устранению.

6. Требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.

7. Привлекать с разрешения руководства сотрудников всех структурных подразделений к решению задач, возложенных на него.

8. Запрашивать лично или через директора «Учреждения» информацию и документы, необходимые для выполнения своих должностных обязанностей.

V. Ответственность

Ответственный несет ответственность:

1. За качество проводимых работ по контролю всех групп пользователей ИСПДн в вопросах обеспечения безопасности персональных данных.

2. За обеспечение устойчивой работоспособности СЗИ ИСПДн.

3. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

4. За правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

VI. Порядок пересмотра инструкции

1. Настоящая Инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

2. С приказом о внесении изменений (дополнений) в настоящую Инструкцию знакомятся под расписку все сотрудники «Учреждения», на которых распространяется действие этой инструкции.

Приложение № 7
к приказу МОУ СОШ № 50
г. Комсомольска-на-Амуре
от 27.08.2015 г. № 265

ИНСТРУКЦИЯ
пользователя ИСПДн по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в МОУ СОШ №50 г. Комсомольска-на-Амуре

I. Назначение и область действия

1. Настоящая инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Муниципального общеобразовательного учреждения средней общеобразовательной школы №50 г.Комсомольска-на-Амуре (далее «Учреждение»), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей настоящей Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

3. Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также на 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.

4. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

II. Порядок реагирования на аварийную ситуацию

1. Действия при возникновении аварийной ситуации:

- В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуации становится возможной в результате реализации одной из угроз, приведенных в таблице «Источники угроз».

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	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
	Телекоммуникационные и ИТ угрозы
16	Сбой системы кондиционирования

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	Физический разрыв внешних каналов связи

- Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

- В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники «Учреждения» (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности системы. Принимаемые меры по возможности согласуются с вышестоящим руководством. По мере необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2. **Уровни реагирования на инцидент:**

При реагировании на инцидент, важно, чтобы пользователь 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 (провыв 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. Обычно к катастрофам относятся обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от объекта.

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

1. **Технические меры:**

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

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

сообщить заместителю директора, курирующему вопросы защиты информации о факте утраты (утере, хищении) документов, содержащих персональные данные. По каждому такому факту назначается служебное расследование.

4. Сотрудникам, допущенным к обработке персональных данных запрещается:

- Сообщать сведения, являющиеся персональными данными, лицам, не имеющим права доступа к этим сведениям.
- Делать неучтенные копии документов, содержащих персональные данные.
- Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.
- Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы.
- Выносить документы, содержащие персональные данные, из помещений «Учреждения» без служебной необходимости.

5. Ответственность сотрудников, допущенных к обработке персональных данных:

- Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и администрацию «Учреждения».
- Контроль за выполнением положений настоящей Инструкции возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
- За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.
- В случае если в результате действий работника был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с главой 39 Трудового кодекса РФ.
- В случае разглашения персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, трудовой договор с работником может быть расторгнут работодателем (подпункт «в» пункта 6 статьи 81 Трудового кодекса РФ).