СОГЛАСОВАНО
Председатель ПК
Л.Г. Костина

УТВЕРЖДАЮ
Ио директора МКОУ Березовская СШ
_____ А.В. Касаткин
приказ от 31.08.2026 № 107

Должностная инструкция заместителя руководителя, ответственного за обеспечение информационной безопасности Муниципальное казенное общеобразовательное учреждение Березовская средняя школа Новоаннинского муниципального района

Волгоградской области

Настоящая должностная инструкция разработана и утверждена в соответствии с положениями указа Президента РФ от 1 мая 2022 г. N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации", постановления Правительства РФ от 15 июля 2022 г. N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)".

1. Общие положения

1.1. Заместитель руководителя, ответственный за обеспечение информационной безопасности, относится к категории специалистов и непосредственно подчиняется директору МКОУ Березовская СШ

1.2. Заместитель руководителя, ответственный за обеспечение информационной безопасности, назначается на должность и освобождается от нее приказом руководителя МКОУ Березовская СШ.

1.3. Заместитель руководителя, ответственный за обеспечение информационной безопасности, осуществляет свою деятельность на основе должностных регламентов (инструкций) федеральных государственных гражданских служащих и государственных гражданских служащих субъекта Российской Федерации, должностных инструкций работников организаций всех форм собственности с учетом особенностей деятельности органа (организации) и подчиняется непосредственно руководителю органа (организации) либо должностному лицу, его замещающему.

1.4. Заместитель руководителя, ответственный за обеспечение информационной безопасности, входит в состав коллегиальных органов органа (организации).

1.5. Указания и поручения заместителя руководителя, ответственного за обеспечение информационной безопасности в части обеспечения информационной безопасности являются обязательными для исполнения всеми работникам МКОУ Березовская СШ.

1.6. Требования к квалификации: высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности.

Заместитель руководителя, ответственный за обеспечение информационной безопасности, на постоянной основе повышает профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

1.7. Для заместителя руководителя, ответственного за обеспечение информационной безопасности, требуется наличие следующих знаний, умений и профессиональных компетенций:

1.7.1. Основные (в том числе производственные, бизнес и управленческие) процессы органа (организации) и специфика обеспечения информационной безопасности органа (организации).

1.7.2. Влияние информационных технологий на деятельность органа (организации), в том числе:

- роль и место информационных технологий (в том числе степень интеграции

информационных технологий) в процессах функционирования органа (организации);

- зависимость основных процессов функционирования органа (организации) от информационных технологий.

1.7.3. Информационно-телекоммуникационные технологии, в том числе:

- современные информационно-телекоммуникационные технологии, используемые в органе (организации);

- способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее - системы и сети), в том числе ограниченного доступа;

- типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

- принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей.

1.7.4. Обеспечение информационной безопасности, в том числе:

- цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;

- цели обеспечения информационной безопасности применительно к основным процессам функционирования органа (организации), реализации и контроля их достижения;

- принципы и направления стратегического развития информационной безопасности в органе (организации);

- правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в органе (организации), состав и содержание таких документов;

- порядок организации работ по обеспечению информационной безопасности в органе (организации);

- основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности органа (организации) для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности органа (организации);

- основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;

- возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

- способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

- порядок организации взаимодействия структурных подразделений органа (организации) при решении вопросов обеспечения информационной безопасности;

- управление проектами по информационной безопасности;

- антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;

- планирование деятельности по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

- формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности органа (организации), подведомственных организаций (филиалов, представительств);

- организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в органе (организации), в подведомственных организациях (филиалах, представительствах) (далее - политика);

- внедрение политики;
- организация контроля и анализа применения политики;
- организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);
- поддержка и совершенствование деятельности по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);
- организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в органе (организации);
- организация внедрения способов и средств для обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);
- организация мероприятий по анализу и контролю состояния информационной безопасности органа (организации) и модернизации (трансформации) процессов функционирования органа (организации) в целях обеспечения информационной безопасности в органе (организации);
- обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;
- организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы органа (организации) и реагированию на компьютерные инциденты;
- организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в органе (организации), подведомственных организациях (филиалах, представительствах).

2. Должностные обязанности

На заместителя руководителя, ответственного за обеспечение информационной безопасности, возлагаются следующие должностные обязанности:

2.1. Участие в формировании политики органа (организации) и согласование стратегии развития органа (организации) в части вопросов обеспечения информационной безопасности.

2.2. Организация разработки политики, направленной в том числе на обеспечение и поддержание стабильной деятельности органа (организации) и его (ее) процессов функционирования в случае проведения компьютерных атак, согласование и утверждение политики в органе (организации), реализация мероприятий, предусмотренных политикой, отслеживание и контроль результатов реализации политики.

2.3. Организация работы по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену.

2.4. Организация реализации и контроля проведения в органе (организации) организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю с учетом меняющихся угроз в информационной сфере, а также самостоятельно ответственным лицом в результате своей деятельности.

2.5. Организация беспрепятственного доступа (в том числе удаленного) должностным лицам

Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим органу (организации) либо используемым органом (организациями), доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет", в целях осуществления мониторинга их защищенности, а также работникам структурного подразделения, осуществляющего функции по обеспечению информационной безопасности.

2.6. Организация взаимодействия с должностными лицами Федеральной службы безопасности Российской Федерации и ее территориальных органов, в том числе контроль исполнения указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами по результатам мониторинга защищенности информационных ресурсов, принадлежащих органу (организации) либо используемых органом (организациями), доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет".

2.7. Организация контроля за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации.

2.8. Организация развития информационной безопасности, формирования и развития навыков работников органа (организации) в сфере информационной безопасности.

2.9. Организация разработки и реализации мероприятий по обеспечению информационной безопасности в органе (организации) в соответствии с требованиями к обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

2.10. Организация контроля пользователей информационных ресурсов органа (организации) в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации.

2.11. Организация планирования мероприятий по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах).

2.12. Организация подготовки правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в органе (организации), осуществление согласования иных документов органа (организации) в части обеспечения информационной безопасности.

2.13. Организация проведения научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах).

2.14. Организация проведения контроля за состоянием обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах), включая оценку защищенности систем и сетей, оператором которых является орган (организация), подведомственные организации (филиалы, представительства).

2.15. Осуществление регулярного контроля текущего уровня (состояния) информационной безопасности в органе (организации), а также реализация мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в органе (организации), в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак.

2.16. Осуществление регулярного и своевременного информирования руководства органа (организации) о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в органе (организации) и результатах практических учений по противодействию компьютерным атакам.

2.17. Осуществление контроля за ведением организационно-распорядительной

документации, статистического учета и отчетности по курируемым разделам работы.

2.18. Осуществление согласования требований к системам и сетям, оператором которых является орган (организация), подведомственные организации (филиалы, представительства), в части обеспечения информационной безопасности.

2.19. Осуществление руководства структурным подразделением органа (организации), обеспечивающим информационную безопасность органа (организации).

2.20. Организация и контроль проведения мероприятий по анализу и оценке состояния информационной безопасности органа (организации) и контроль их результатов.

2.21. Организация и контроль функционирования системы обеспечения информационной безопасности в органе (организации), координация функционирования систем обеспечения информационной безопасности в подведомственных организациях (филиалах, представительствах).

2.22. Координация деятельности иных структурных подразделений органа (организации), подведомственных организаций (филиалов, представительств) по вопросам обеспечения информационной безопасности.

2.23. Согласование политики, технического задания и иной основополагающей документации в сфере информационных технологий, цифровизации и цифровой трансформации органа (организации).

2.24. Организация с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации обнаружения, предупреждения и ликвидации последствий компьютерных атак, реагирования на компьютерные инциденты с информационными ресурсами органа (организации), а также взаимодействия с Национальным координационным центром по компьютерным инцидентам одним (или несколькими) из следующих способов:

- силами структурного подразделения, ответственного за обеспечение информационной безопасности, с заключением соглашения (издания совместного акта) о взаимодействии с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам), включающего в том числе права и обязанности сторон, порядок проведения совместных мероприятий, регламент информационного обмена, порядок и сроки представления отчетности, порядок и формы контроля;

- силами структурного подразделения, ответственного за обеспечение информационной безопасности, с его аккредитацией как центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

- силами организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2.25. Обеспечение планирования и реализации мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 указа Президента РФ от 1 мая 2022 г. N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

2.26. Сопровождение мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

2.27. Проведение работы по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в органе (организации), подведомственных организациях (филиалах, представительствах).

2.28. Принятие мер по совершенствованию обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах).

2.29. Соблюдение и обеспечение выполнения законодательства Российской Федерации.

2.30. Согласование политики органа (организации) с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в случаях, установленных законодательством Российской Федерации.

2.31. Представление по запросам Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю достоверных сведений о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в органе (организации).

2.32. Поддержание уровня квалификации и постоянное развитие своих навыков в области информационной безопасности, необходимых для обеспечения информационной безопасности в органе (организации).

2.33. Проведение и участие в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций.

2.34. Участие в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

3. Права

Заместитель руководителя, ответственный за обеспечение информационной безопасности имеет право:

3.1. Давать указания и поручения работникам органа (организации) в части обеспечения информационной безопасности.

3.2. Запрашивать от работников органа (организации) информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей.

3.3. Участвовать в заседаниях (совещаниях) коллегиальных органов органа (организации), принятии решений по вопросам деятельности органа (организации), а также по внесению предложений по совершенствованию деятельности органа (организации).

3.4. Участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу органа (организации).

3.5. Представлять результаты реализации политики коллегиальному органу (органа) организации.

3.6. Принимать решения по вопросам обеспечения информационной безопасности органа (организации).

3.7. Взаимодействовать с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности.

3.8. Вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности.

3.9. Инициировать проверки уровня (состояния) обеспечения информационной безопасности в органе (организации), ее подведомственных и дочерних организациях.

3.10. Организовывать на объектах органа (организации) мероприятия по информационной безопасности, разработку и представление руководителю органа (организации) предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий.

3.11. Получать доступ в установленном порядке к сведениям, составляющим

государственную тайну, если исполнение обязанностей ответственного лица связано с использованием таких сведений и наличием необходимых прав и полномочий.

3.12. Получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы, органы местного самоуправления, общественные объединения и другие организации.

3.13. Обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей ответственного лица.

3.14. На все предусмотренные законодательством Российской Федерации социальные гарантии.

4. Ответственность

Заместитель руководителя, ответственный за обеспечение информационной безопасности, несет ответственность за:

4.1. Неисполнение или ненадлежащее исполнение своих обязанностей.

4.2. Действия (бездействие), ведущие к нарушению прав и законных интересов органа (организации).

4.3. Разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей.

4.4. Достижение целей обеспечения информационной безопасности.

4.5. Поддержание и непрерывное развитие информационной безопасности органа (организации) для исключения (невозможности реализации) негативных последствий.

4.6. Организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности органа (организации).

4.7. Нарушения требований по обеспечению информационной безопасности.

4.8. Нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.

С инструкцией ознакомлен:

_____