Приложение № 1 к приказу
№___ от _____
об утверждении должностной
инструкции администратора
локальной вычислительной сети

Должностная инструкция администратора локальной вычислительной сети

1. Общие положения

Настоящая инструкция определяет функциональные обязанности, права и ответственность администратора локальной вычислительной сети (далее по тексту - ЛВС).

1.1. Администратор ЛВС назначается и освобождается от занимаемой должности приказом директора МБОУ Великооктябрьская СОШ.

1.2. Администратор ЛВС назначается из числа работников МБОУ Великотябрьская СОШ.

1.3. Непосредственное руководство администратором ЛВС осуществляет директор МБОУ Великооктябрьская СОШ.

2. Задачи администратора ЛВС.

2.1. Основными задачами администратора ЛВС являются:

- системное администрирование ЛВС МБОУ Великооктябрьская СОШ;
- осуществление бесперебойного и качественного функционирования аппаратных средств информационной системы МБОУ Великооктябрьская СОШ;
- защита локальной вычислительной сети от несанкционированного доступа, регулирование прав доступа пользователей сети к ресурсам ЛВС.
- обеспечение защиты информации МБОУ Великооктябрьская СОШот утечки по техническим каналам при её обработке, хранении и передаче по каналам связи.
- решение вопросов информационной безопасности МБОУ Великооктябрьская СОШ;

2.2. В своей деятельности администратор ЛВС руководствуется следующими документами:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Руководящими документами Гостехкомиссии и ФСТЭК России по защите конфиденциальной информации и обеспечению информационной безопасности;

- Локальными документами организации, регламентирующими обработку персональных данных (Положения, инструкции, правила);
- Должностной инструкцией.

2.3. Для осуществления своей деятельности администратор ЛВС имеет право доступа во все помещения, где установлены средства автоматизированной обработки информации, телекоммуникационные устройства и средства связи.

2.4. Администратор ЛВС обязан производить административные действия со строго определенных доверенных станций, оснащенных средствами защиты от несанкционированного доступа и располагающихся в помещениях с ограниченным доступом.

2.5. При контактах с пользователем решение об идентификации обратившегося лица администратор ЛВС принимает любым доступным для него способом.

2.6. Все журналы и документы по безопасности администратор ЛВС хранит в электронном виде не менее трех лет, если иное не указано явно в технологической схеме, причем ежегодно и по требованию контролирующих органов должна производиться их распечатка на бумажном носителе. Копии журналов на бумажных носителях хранятся у системного администратора в течение года.

3. Обязанности администратора ЛВС

3.1. Администратор ЛВС самостоятельно работает на основе уверенного знания основных параметров, требований, правил установки, способов выявления и устранения неполадок сетевых операционных систем и пользовательских сред, умеет квалифицированно работать с ними.

3.2. Устанавливает на серверы, рабочие станции и персональные компьютеры пользовательские программы и сетевые программы. Организует рабочие места для пользователей. Осуществляет контроль монтажа и пусконаладочных работ оборудования специалистами сторонних организаций.

3.3. Конфигурирует и оптимизирует сеть и серверы, разрабатывает и вносит на рассмотрение своего непосредственного руководителя предложения по оптимизации и развитию сети, в том числе по приобретению оборудования.

3.4. Обеспечивает бесперебойную работу серверов, сети и персональных компьютеров. Поддерживает рабочее состояние программного обеспечения серверов, рабочих станций, персональных компьютеров пользователей, подключенных и неподключенных к сети, принтеров, факсов, в том числе разрабатывает и реализует систему профилактических мер. Обеспечивает интегрирование программного обеспечения управления базами и потоками данных сервера и рабочих станций.

3.5. Обеспечивает:

- сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных);
- безопасность межсетевого взаимодействия.

3.6. Принимает исчерпывающие меры по недопущению возникновения неполадок в сети.

3.7. Самостоятельно устраняет неполадки в работе оборудования и программного обеспечения сети, сервера, персональных компьютеров.

3.8. В случае невозможности устранения неполадок в работе компьютеров, сервера, сети своими силами - привлекает специалистов сервисных организаций для устранения неисправностей сетевого

оборудования. При этом активно участвует в восстановлении работоспособности указанных систем.

3.9. Обучает пользователей работе в сети, ведению архивов; консультирует пользователей по вопросам использования компьютеров, общесистемного программного обеспечения, сетевых ресурсов; разрабатывает необходимые инструкции, методические рекомендации и другие разъяснительные материалы и доводит их до сведения пользователей.

3.10. Ведет журнал учета нерегламентированного программного обеспечения (приложение к настоящей инструкции), оформляет иную техническую документацию.

3.11. Принимает, исчерпывающие меры по сохранению данных, в том числе в случае возникновения неполадок в сети, на сервере, в отдельных компьютерах, в том числе обеспечивает своевременное копирование и резервирование данных.

3.12. Контролирует использование сетевых ресурсов и дискового пространства, выявляет ошибки пользователей и неполадки сетевого программного обеспечения. Сообщает своему непосредственному руководителю о случаях злоупотребления сетью и принятых мерах.

3.13. Участвует в разработке исходных данных и постановке задач на модернизацию компьютерной сети.

3.14. Разрабатывает способы и методы организации доступа пользователей компьютерной сети к ресурсам компьютерной сети.

3.15. Предотвращает несанкционированные модификации программного обеспечения, добавления новых функций, несанкционированный доступ к информации, аппаратуре и другим общим ресурсам компьютерной сети. В случае обнаружения модификаций или нерегламентированного программного обеспечения фиксирует событие в журнале учета обнаружения нерегламентированного программного" обеспечения, ставит в известность руководителя - структурного подразделения, где произошло событие, администратора информационной безопасности и совместно с ним проводит соответствующее расследование.

3.16. Решает вопросы информационной безопасности школы.

3.17. Осуществляет учет и периодический контроль за составом и полномочиями пользователей различных объектов вычислительной техники (далее – ОВТ) и информационных систем (далее – ИС).

3.18. Периодически проверяет состояние используемых систем защиты информации от несанкционированного доступа (далее – НСД), осуществляет проверку правильности их настройки.

3.19. Докладывает руководителю об имевших место попытках несанкционированного доступа к информации и ОВТ.

3.20. Проводит работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации ОВТ.

3.21. Контролирует своевременное и точное отражение изменений в организационно-распорядительных и нормативных документах по управлению информационной безопасностью.

3.22. Разрабатывает инструкции и памятки для пользователей, обрабатывающих персональные данные (далее - ПДн).

3.23. Проводит периодическое тестирование функций систем защиты ПДн при изменении программной среды и персонала информационных систем персональных данных.

3.24. Соблюдает требования режима конфиденциальности информации, содержащей персональные данные работников, обучающихся, а также третьих лиц, ставшей ему известной в связи с исполнением своих должностных обязанностей, и не использовать ее в интересах, не связанных с исполнением указанных обязанностей.

3.25. Проводит работы по установке и настройке межсетевых экранов.

3.26. Разрабатывает регламенты проведения работ по обеспечению безопасности персональных данных.

3.27. Обеспечивает разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации.

3.28. Обеспечивает учет и надежное хранение носителей конфиденциальной информации, исключающее несанкционированный доступ к ним, их хищение, подмену и уничтожение.

3.29. Обеспечивает ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и телекоммуникационное оборудование, а также хранятся носители информации.

3.30. Обеспечивает разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации

3.31. Осуществляет регистрацию действий пользователей информационной системы, контроль несанкционированного доступа и действий пользователей и посторонних лиц.

3.32. Осуществляет контроль за размещением средств отображения информации, исключающее её несанкционированный просмотр.

3.33. Осуществляет запрет работы на рабочих станциях и серверах посторонних лиц.

3.34. Осуществляет периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты.

3.35. Осуществляет периодические проверки в части соблюдения установленных требований к защите персональных данных согласно плану внутренних проверок состояния защиты персональных данных (Приложение №3 к Положению о персональных данных) и ведёт журнал проверок (Приложение №6 к Положению о персональных данных персональных данных).

4. Ответственность

4.1. На администратора ЛВС возлагается ответственность за работу локальной вычислительной сети, серверов, рабочих станций, программно - технических и криптографических средств защиты информации и за качество проводимых работ по обеспечению защиты информации на ОВТ в соответствии с функциональными обязанностями;

4.2. Администратор ЛВС несет ответственность по действующему законодательств за разглашение сведений, составляющих (государственную, банковскую, коммерческую) тайну, и сведений ограниченного распространения, ставших известными ему по роду работы;

4.3. Администратор ЛВС несет ответственность за реализацию принятой в школе политики безопасности, утвержденной приказами директора МБОУ Великооктябрьская СОШ, плану мероприятий по организации защиты персональных данных.

5. Права

5.1. Администратор ЛВС имеет право:

5.2. Знакомиться с решениями руководства, касающимися его деятельности.

5.3. Сообщать своему непосредственному руководителю о всех выявленных в процессе своей деятельности недостатках и вносить предложения по их устранению.

5.4. Требовать от руководства создания нормальных условий для выполнения служебных обязанностей.

5.5. Принимать решения в пределах своей компетенции.

5.6. Требовать доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты;

5.7. Участвовать в проведении служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС;

5.8. Непосредственно обращаться к руководителю с требованием прекращения работы в ИС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;

5.9. Вносить свои предложения по совершенствованию мер защиты информации в СОШ.

Приложение №1 к инструкции администратора ЛВС,
утвержденной приказом №___ от_____

Журнал учета обнаружения нерегламентированного программного обеспечения

Журнал начат: « »_____20 г.
Должность_____
/Ф.И.О. должностного лица/

Журнал завершен: « »_____20 г.
Должность_____
/Ф.И.О. должностного лица/

№ п/п	Дата обнаружения	Где обнаружено (№ кабинета)	Ф.И.О. работника	Наименование нерегламентированного ПО	Принятые меры	Подпись	Примечания