Приложение №2
к приказу от 31.12.2019 г. № 104/06-од
«О назначении ответственного
за организацию обработки персональных
данных и администраторов безопасности»

УТВЕРЖДЕНО
приказом ГБОУ гимназии №1
г. Новокуйбышевска
от 31.12.2019 г. № 104/06-од
Директор
Л.Г. Слепцова

ИНСТРУКЦИЯ

администратора безопасности в информационной системе (ИС)

ГБОУ гимназии №1 г. Новокуйбышевска

1. Общие положения

1.1. Администратор безопасности в ИС (далее – Администратор) назначается приказом руководителя (директора) государственного бюджетного общеобразовательного учреждения Самарской области гимназии № 1 им. Н.И. Ферапонтова города Новокуйбышевска городского округа Новокуйбышевск Самарской области (сокращенно - ГБОУ гимназия № 1 г. Новокуйбышевска) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) и другой конфиденциальной информации в процессе ее обработки в ИС ГБОУ гимназии № 1 г. Новокуйбышевска («Бухгалтерия», «Кадры», «АСУ РСО электронный журнал/дневник», «Образование»).

1.2.Администратор обязан поддерживать в актуальном состоянии свои знания законодательных, нормативно-правовых актов Российской Федерации и методических материалов в сфере обработки и защиты ПДн.

1.3.В своей деятельности Администратор руководствуется настоящей Инструкцией, Положением об обработке и защите персональных данных, Политикой информационной безопасности и действующим

законодательством в сфере защиты персональных данных и конфиденциальной информации.

1.4.Администратор безопасности подчиняется напрямую руководителю (директору образовательной организации) и Ответственному за организацию обработки персональных данных, имеет право требовать от пользователей ИС выполнения указаний и инструкций, связанных с защитой информации.

1.5.Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней

защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. Функции и обязанности Администратора безопасности в ИС

2.1.Изучение особенностей и технологических процессов обработки информации в ГБОУ гимназии №1 г. Новокуйбышевска с целью принятия решения о необходимости защиты информации в ИС и классификации ИС, либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации об ИС сотрудниками сторонней организации. По окончании аналитических работ Администратор обязан ознакомиться с их результатами и подписать отчетные документы, либо составить мотивированный отказ в подписании таких документов и отправить их на доработку сторонней организации.

2.2.Определение актуальных угроз безопасности информации и разработка документа «Модель угроз безопасности ИС», либо привлечение на договорной основе сторонних организаций для таких работ.

2.3.Периодический пересмотр актуальных угроз безопасности информации в следующих случаях:

- ежегодный плановый пересмотр актуальных угроз безопасности информации;
- появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки в ГИС;
- существенное изменение условий функционирования ГИС, внедрение новых технологий;

- изменение нормативной документации, касающейся моделирования угроз безопасности информации;
- в результате инцидента безопасности.

2.4.Участие в подготовке технических заданий для конкурсов и аукционов, связанных с закупкой технических средств, программного обеспечения или средств защиты информации для ИС.

2.5.Выработка предложений руководителю (директору) ГБОУ гимназии №1 г. Новокуйбышевска по совершенствованию системы защиты информации в ИС.

2.6.Ведение учета применяемых в ИС средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.

2.7.Знание состава, структуры, назначения и выполняемых задач ИС, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку ПДн и иной конфиденциальной информации.

2.8.Обеспечение передачи конфиденциальной информации и персональных данных через сети связи общего пользования в зашифрованном виде.

2.9.Участие в разработке плана мероприятий по обеспечению безопасности защищаемой информации в ИС. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в ИС и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.

2.10. Осуществление контроля неизменности состояния аттестованной ИС (расположение и состав технических средств, состав программного обеспечения, физическое и логическое строение сети). В случае планирования изменения условий функционирования ИС, Администратор должен связаться с аттестующим органом и получить указания к дальнейшим действиям.

2.11. Осуществление контроля физической сохранности и целостности технических средств ИС, а также контроль сохранности и целостности программно-аппаратных средств защиты информации. Контроль неизменности состава технических средств в ИС.

2.12.Организация учета съемных носителей информации. Настройка соответствующих программных механизмов средств защиты информации для запрета неучтенных съемных носителей.

2.13.Проведение инструктажей сотрудников, работающих с защищаемой информацией в ИС (далее – Пользователи ИС), по темам: правила работы в ИС, защита информации в ИС, положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников ГБОУ гимназии №1 г. Новокуйбышевска в вопросах информационной безопасности.

2.14.Организация первоначального доступа пользователям ИС к ресурсам информационный системы в соответствии с утвержденным Положением о разграничении прав доступа в ИС. Блокировка учетных записей, изменение полномочий пользователей и добавление новых пользователей ИС.

2.15.Осуществление резервного копирования защищаемой информации.

2.16.Осуществление контроля целостности программного обеспечения (в том числе и средств защиты информации).

2.17.По мере возможности, Администратор должен восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а также восстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.

2.18.Контроль выполнения Пользователями ИС требований Инструкции пользователя ИС, а также других установленных требований для обеспечения безопасности ПДн и иной конфиденциальной информации.

2.19.В случае получения от Пользователей ИС информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, Администратор незамедлительно принимает все необходимые меры для обеспечения безопасности ПДн и иной конфиденциальной информации в пределах своих полномочий.

2.20.Контроль обновлений системного, прикладного программного обеспечения и средств защиты информации (в том числе обновлений антивирусных баз).

2.21.Контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств ИС или настройку/установку программного обеспечения ИС.

2.22.Обеспечение функционирования и поддержания работоспособности в ИС:

- системы криптографической защиты информации;
- системы антивирусной защиты.

2.23.Обеспечение непрерывности процессов в ИС. В случае нарушения работоспособности технических средств и программного обеспечения ИС, в том числе средств защиты ИС, Администратор принимает меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

2.24.Своевременное информирование Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ГИС.

3. Права Администратора безопасности ИС

Администратор имеет право:

3.1.Знакомиться с нормативными актами ГБОУ гимназии №1 г. Новокуйбышевска, регламентирующими процессы обработки и защиты ПДн и иной конфиденциальной информации.

3.2.Вносить предложения руководителю (директору) ГБОУ гимназии №1 г. Новокуйбышевска по совершенствованию существующей системы защиты информации.

3.3.Требовать от Пользователей ИС соблюдения требований Инструкции пользователя ИС и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн и иной конфиденциальной информации.

3.4.Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн и иной конфиденциальной информации.

3.5.Требовать прекращения работы в ИС, как в целом, так и отдельных Пользователей ИС, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИС.

3.6.Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

4. Рабочее место Администратора безопасности ИС

4.1.Одним из ключевых элементов системы защиты информации в ИС является АРМ Администратора.

4.2.АРМ Администратора устанавливается таким образом, чтобы исключался как преднамеренный, так и непреднамеренный несанкционированный доступ к техническим средствам АРМ Администратора.

4.3.На АРМ Администратора устанавливаются средства централизованного управления:

- системы криптографической защиты информации;
- системы антивирусной защиты ИС.

4.4.Администратор осуществляет централизованное управление политиками безопасности в ИС, обновлениями средств защиты информации, обновлениями антивирусных баз.

4.5.Рабочее место Администратора является объектом защиты и защищается согласно требованиям к тому же классу, по которому классифицирована ИС в целом.

5. Обслуживание средств криптографической защиты информации

5.1.Общие правила работы с криптосредствами описаны в утвержденной Инструкции по обеспечению безопасности эксплуатации СКЗИ. В данном

разделе описана часть, касающаяся функций и обязанностей Администратора.

5.2.Исходя из требований к защите информации и актуальных угроз безопасности информации в ИС, Администратор определяет необходимость использования средств криптографической защиты информации (далее – СКЗИ) в системе защиты информации ИС.

5.3.Администратор обеспечивает соответствие работы с СКЗИ технической и эксплуатационной документации к ним.

5.4.Администратор осуществляет учет СКЗИ.

5.5.Администратор контролирует передачу СКЗИ, ключевой информации пользователям ИС.

5.6.Администратор обеспечивает хранение дистрибутивов СКЗИ в шкафах (сейфах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.7.Администратор обеспечивает раздельное хранение действующих и резервных ключевых документов.

5.8.Администратор производит инструктаж пользователей перед работой с СКЗИ. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности.

5.9.Администратор составляет и поддерживает в актуальном состоянии список лиц, допущенных к работе с СКЗИ.

5.10. Администратор осуществляет проверку готовности СКЗИ к использованию в ходе проведения проверок согласно Плану мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ИС.

5.11. Администратор принимает участие в составе комиссии расследования попыток посторонних лиц получить сведения об используемых СКЗИ, случаев утраты дистрибутивов СКЗИ, ключевой информации и эксплуатационной документации к СКЗИ, ключей от помещений и хранилищ СКЗИ.

5.12. Администратор в составе комиссии по уничтожению принимает участие в уничтожении ключевой информации и документов. Уничтожение ключевой информации производится путем физического уничтожения ключевого носителя или путем гарантированного затирания ключевой информации.

6. Настройка и обслуживание системы антивирусной защиты

6.1.Общие правила работы с системой антивирусной защиты описаны в утвержденной Инструкция по организации антивирусной защиты. В данном разделе описана часть, касающаяся функций и обязанностей Администратора.

6.2.Исходя из требований к защите информации и актуальных угроз безопасности информации в ИС, Администратор определяет необходимость использования системы антивирусной защиты в системе защиты информации ИС.

6.3.Администратор осуществляет учет антивирусной защиты.

6.4.Администратор контролирует установку антивирусной защиты пользователям ИС.

6.5.Администратор производит инструктаж пользователей перед работой с антивирусной защитой. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности.

6.6.Администратор составляет и поддерживает в актуальном состоянии список лиц, допущенных к работе с антивирусной защитой.

6.7.Администратор осуществляет проверку готовности антивирусной защиты к использованию в ходе проведения проверок согласно Плану мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ИС.

6.8.Администратор принимает участие в составе комиссии расследования попыток посторонних лиц получить сведения об используемой антивирусной защите.

6.9.Администратор в составе комиссии по уничтожению принимает участие в уничтожении информации об антивирусной защите и уничтожения ключевого носителя путем гарантированного затирания ключевой информации.

7. Регистрация и учет событий безопасности

7.1.Под системой регистрации и учета событий безопасности в ИС понимается совокупность средств централизованного управления всех СЗИ в ИС.

7.2.Система регистрации и учета событий безопасности, а также информация, хранящаяся в электронных журналах регистрации событий сами по себе являются объектами защиты. Доступ к записям системы регистрации и учета событий безопасности разрешен только Администратору.

7.3.Администратор периодически изучает записи системы регистрации и учета событий безопасности и в случае обнаружения инцидентов безопасности информации сообщает об этом руководителю (директору) ГБОУ гимназии №1 г. Новокуйбышевска.

7.4.Администратор изучает журналы событий с определенной периодичностью.

8. Действия Администратора при ремонте технических средств, обслуживании программного обеспечения и утилизации носителей информации

8.1.Администратор присутствует в процессе установки, обновления, настройки программного обеспечения в ИС (в том числе и средств защиты информации) сотрудниками сторонних организаций.

8.2.Администратор присутствует в процессе ремонта технических средств ИС сотрудниками сторонних организаций.

8.3.Администратор обеспечивает гарантированное затирание данных с носителей информации, либо демонтаж носителей информации (в том числе

и оперативной памяти) с технических средств в случае необходимости отправки технических средств для ремонта на территорию сторонних организаций.

8.4.Администратор обеспечивает гарантированное затирание данных на машинных носителях информации при утилизации технических средств, либо принимает участие в физическом уничтожении машинных носителей информации в составе комиссии по уничтожению.