Российская Федерация
Министерство образования Кировской области
**Гимназия №1 г. Кирово-Чепецка**

г. Кирово-Чепецк, просп. Мира, 52. ☎ Тел 5-31-42; 5-40-93; 5-41-05;5-19-18
факс (83361) 5-31-42, эл. почта gimns1@mail.ru; сайт www.gimns.org

# П Р И К А З

10.08.2021 г. № 236

***О назначении специалистов по защите и безопасности информации***

В соответствии с «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2012 № 282,

**ПРИКАЗЫВАЮ:**

1. Назначить Зорина А.В., инженера – программиста, Скрябина С.Ю., инженера – программиста, специалистами по защите и безопасности информации (далее-специалист по защите и безопасности информации) в КОГОАУ «Гимназия №1».
2. Возложить на работников, указанных в п. 1 настоящего приказа, следующие функции:
-администрирование информационных систем персональных данных (АС);
-администрирование средств антивирусной защиты информационных систем персональных данных (АС);
-администрирование средств и систем защиты персональных данных в информационных системах персональных данных (АС).
3. Утвердить инструкцию специалиста администратора безопасности информации.
4. Контроль за выполнением требований настоящего приказа возложить на Сычугову С.Ю., заместителя директора.

**Директор**
**КОГОАУ «Гимназия №1»** **А.П.Ходырев**

Ходырев Александр Петрович

Подписан: Ходырев Александр Петрович
DN: C=RU, S=Кировская область, L=город Кирово-Чепецк, T=Директор, O="КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ""ГИМНАЗИЯ №1 Г. КИРОВО-ЧЕПЕЦКА""", СНИЛС=06054165433, ИНН=431205860506, E=gimns1@mail.ru, G=Александр Петрович, SN=Ходырев, CN=Ходырев Александр Петрович
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2023-02-07 10:46:16
Foxit Reader Версия: 9.7.0

**Утверждена приказом по КОГОАУ «Гимназия №1»**
**от 10.08.2021 г. №_____**

# ИНСТРУКЦИЯ

## специалиста по защите и безопасности информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности должностного лица, ответственного за обеспечение защиты и безопасности информации (в том числе персональных данных (ПДн), обрабатываемой в информационных системах ПДн (ИСПДн) _____, далее - (администратора безопасности).

1.2. Действие настоящей Инструкции распространяется на структурные подразделения _____.

1.3. Администратор безопасности назначается приказом руководителя _____ из числа подготовленных работников подразделения информационной безопасности (ИБ).

1.4. Администратор безопасности по вопросам обеспечения безопасности информации подчиняется руководителю подразделения ИБ, являющемуся структурным подразделением, назначаемым ответственным за обеспечение безопасности информации в _____.

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

1.6. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ИСПДн _____в вопросах обеспечения безопасности информации.

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

1.8. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн _____, состояние и поддержание установленного уровня защиты информации, обрабатываемой в ИСПДн _____.

2. ЗАДАЧИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Основными задачами администратора безопасности являются:

- поддержание необходимого уровня защиты ИСПДн _____ от несанкционированного доступа (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 (СЗИ) от НСД и основных технических средств и систем (ОТСС) ИСПДн _____;

- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;

- оперативное реагирование на нарушения требований по ИБ в ИСПДн _____ и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности осуществляет:

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

- текущий контроль технологического процесса автоматизированной обработки ПДн;

- 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 _____ и территориальных органах _____;

- методическую помощь всем работникам _____ и территориальных органов _____ по вопросам обеспечения безопасности ПДн.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Администратор безопасности обязан:

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

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 _____ согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

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

3.6. Вести контроль осуществления резервного копирования информации.

3.7. Анализировать состояние защиты ИСПДн _____.

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 _____ введенного режима безопасности, а также правильность работы с элементами ИСПДн и

средствами защиты информации.

3.11. Контролировать исполнение пользователями правил парольной политики.

3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

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

3.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) ИСПДн _____.

3.15. Оказывать помощь пользователям ИСПДн _____ в части применения средств защиты и консультировать по вопросам введенного режима защиты.

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

3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн _____, в том числе средств защиты, 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 _____ требованиям безопасности информации <1>.

---

<1> Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных", Постановление Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", нормативно-правовые акты и методические документы ФСТЭК России и ФСБ России по защите персональных данных при их обработке в информационных системах персональных данных.

4. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности имеет право:

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

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

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

4.4. Организовывать и участвовать в любых проверках по использованию пользователями _____ и территориальных органов _____ телекоммуникационных ресурсов.

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

4.6. Осуществлять взаимодействие с руководством и персоналом _____ и территориальных органов _____ 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 Руководителей и специалистов структурных подразделений _____ и территориальных органов _____ информацию и материалы, необходимые для организации своей работы.

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

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности несет ответственность <2>:

---

<2> Виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

5.1. За организацию защиты информационных ресурсов и технических средств ИСПДн _____.

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ИСПДн _____.

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

6. ДЕЙСТВИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НСД

6.1. К попыткам НСД относятся:

- сеансы работы с телекоммуникационными ресурсами _____ и территориальных органов _____ 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 _____ 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 руководству подразделения ИБ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

- известить Руководителя структурного подразделения _____ и/или территориальных органов _____, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

- проанализировать характер НСД;

- по решению руководства подразделения ИБ осуществить действия по выяснению причин, приведших к НСД;

- предпринять меры по предотвращению подобных инцидентов в дальнейшем.