ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ШКОЛА – ИНТЕРНАТ № 37 ФРУНЗЕНСКОГО РАЙОНА САНКТ - ПЕТЕРБУРГА

П Р И К А З

от 26.03.2024 **№ 23/3-ОД**

О назначении администратора безопасности информации в государственном бюджетном общеобразовательном учреждении школе-интернате № 37 Фрунзенского района Санкт-Петербурга

В соответствии с составов и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных утвержденным Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

П Р И К А З Ы В А Ю :

1. Назначить администратором безопасности информации в государственном бюджетном общеобразовательном учреждении школе-интернате №37 Фрунзенского района Санкт-Петербурга (далее – администратор безопасности информации) *инженера Кириллова Б.А*.
2. Утвердить Инструкцию администратора безопасности информации согласно приложению.
3. Контроль за выполнением настоящего приказа оставляю за собой.

Директор О.А.Орлова

Приложение
к приказу
от 26.03.2024 №23/3-ОД

ИНСТРУКЦИЯ
администратора безопасности информации
в государственном бюджетном общеобразовательном учреждении школе-интернате №37 Фрунзенского района Санкт-Петербурга

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности должностного лица, ответственного за обеспечение безопасности информации в государственном бюджетном общеобразовательном учреждении школе-интернате №37 Фрунзенского района Санкт-Петербурга (далее – Администратор безопасности информации), в том числе персональных данных (далее – ПДн), обрабатываемой в информационных системах ПДн (далее – ИСПДн) в государственном бюджетном общеобразовательном учреждении школе-интернате №37 Фрунзенского района Санкт-Петербурга (далее – ГБОУ №37).

1.2. Действие настоящей Инструкции распространяется на все подразделения ГБОУ №37.

1.3. Администратор безопасности информации назначается приказом ГБОУ №37.

1.4. Администратор безопасности информации по вопросам обеспечения безопасности информации подчиняется *директору* ГБОУ №37.

1.5. Администратор безопасности информации отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн в ГБОУ №37.

1.6. Администратор безопасности информации осуществляет методическое руководство деятельностью пользователей ИСПДн ГБОУ №37 по вопросам обеспечения безопасности информации.

1.7. Требования администратора безопасности информации, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн ГБОУ №37.

1.8. Администратор безопасности информации несет персональную ответственность за качество проводимых им работ по контролю действий должностных лиц ГБОУ №37 (далее – Пользователи) при работе в ИСПДн ГБОУ №37, состояние и поддержание установленного уровня защищенности информации, обрабатываемой в ИСПДн ГБОУ №37.

2. Задачи Администратора безопасности информации

2.1. Основными задачами Администратора безопасности информации являются:

поддержание необходимого уровня защищенности ИСПДн ГБОУ №37 от несанкционированного доступа (далее – 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 (далее – СЗИ) от НСД и основных технических средств и систем (далее – ОТСС) ИСПДн ГБОУ №37,

периодическое обновление СЗИ и проведение комплекса мероприятий по предотвращению нарушений требований информационной безопасности (далее – ИБ),

оперативное реагирование на нарушения требований по ИБ в ИСПДн ГБОУ №37 и участие в их предотвращении (нейтрализации).

2.2. В рамках выполнения основных задач администратор безопасности информации 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 ГБОУ №37,

методическую помощь пользователям ИСПДн ГБОУ №37 по вопросам обеспечения безопасности ПДн.

3. Обязанности администратора безопасности информации

Администратор безопасности информации обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн ГБОУ №37.

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 ГБОУ №37 согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн ГБОУ №37 при обработке ПДн.

3.6. Вести контроль осуществления резервного копирования информации.

3.7. Анализировать состояние защиты ИСПДн ГБОУ №37.

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 ГБОУ №37 введенного режима безопасности, а также правильность работы с элементами ИСПДн ГБОУ №37 и средствами защиты информации.

3.11. Контролировать исполнение пользователями ИСПДн ГБОУ №37 правил парольной политики.

3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей ИСПДн ГБОУ №37 и выявления возможных нарушений.

3.13. Не допускать установку, использование, хранение и размножение в ИСПДн ГБОУ №37 программных средств, не связанных с выполнением функциональных задач.

3.14. Осуществлять периодические контрольные проверки автоматизированных

рабочих мест ИСПДн ГБОУ №37.

3.15. Оказывать помощь пользователям ИСПДн ГБОУ №37 в части применения СЗИ и консультировать по вопросам введенного режима защиты.

3.16. Периодически представлять руководству отчет о состоянии СЗИ ИСПДн ГБОУ №37, о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн ГБОУ №37, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.18. В случае выявления нарушений режима безопасности информации, 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 ГБОУ №37 требованиям безопасности информации.

4. Права администратора безопасности информации

Администратор безопасности информации имеет право:

4.1. Отключать от ресурсов ИСПДн ГБОУ №37 пользователей, осуществивших НСД к защищаемым ресурсам ИСПДн ГБОУ №37 или нарушивших другие требования по ИБ.

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

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, несанкционированного доступа, утраты, порчи защищаемой информации и технических средств ИСПДн ГБОУ №37.

4.4. Организовывать и участвовать в любых проверках по использованию пользователями ГБОУ №37 телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн ГБОУ №37 при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с руководством и персоналом ГБОУ №37 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 пользователей ИСПДн ГБОУ №37 информацию и материалы, необходимые для организации своей работы.

4.9. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ ПДн, обрабатываемых в ГБОУ №37.

5. Ответственность администратора безопасности информации

Администратор безопасности несет ответственность за:

5.1. Организацию защиты информационных ресурсов и технических средств ИСПДн ГБОУ №37.

5.2. Качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защищенности информационных и технических ресурсов ИСПДн ГБОУ №37.

5.3. Разглашение сведений ограниченного доступа, ставших известными ему по роду работы.

6. Действия администратора безопасности информации при обнаружении попыток НСД

6.1. К попыткам НСД относятся:

сеансы работы с телекоммуникационными ресурсами ГБОУ №37 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 ГБОУ №37 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 *директору* ГБОУ №37 *(согласно п. 1.4)* о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях,

известить руководителя ГБОУ №37, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД,

проанализировать характер НСД,

по решению ответственного за защиту информации в ГБОУ №37 осуществить действия по выяснению причин, приведших к НСД,

предпринять меры по предотвращению подобных инцидентов в дальнейшем.