Приложение № 2

**РУКОВОДСТВО**

**АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ**

**РЕСУРСОВ ОБЪЕКТА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ –**

**ИСПДН ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. В.Г. ШУХОВА»**

**2021 г.**

# Общие положения

1.1. Администратор безопасности ИСПДн назначается приказом (распоряжением) Руководителя.

1.2. Администратор подчиняется Руководителю.

1.3. Администратор в своей работе руководствуется настоящей инструкцией и Политикой безопасности ПДн, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами Оператора».

1.4. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности является ответственным должностным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании ФГБОУ ВО «БГТУ им. В.Г. Шухова», чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а также средствами контроля за техническими средствами защиты.

1.8. Администратор безопасности осуществляет методическое руководство Операторов и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.9. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

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

# Должностные обязанности

Администратор безопасности обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.11. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

2.13. Контролировать исполнение пользователями парольной политики.

2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

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

2.17. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

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

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

2.21. 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.

2.22. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

**3. Права и ответственность**

3.1 Администратор безопасности ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн, в том числе производить установку и настройку элементов средств защиты ИСПДн, контролировать и поддерживать их работоспособность и выполнять прочие действия в рамках должностных обязанностей.

3.2. Администратор безопасности ИСПДн имеет право останавливать обработку защищаемой информации в ИСПДн в случае нарушения пользователями установленных порядка и правил обеспечения информационной безопасности.

3.2 Администратор ИСПДн, виновный в несоблюдении Настоящей инструкции расценивается как нарушитель Федерального закона РФ 27.07.2006 г. № 152-ФЗ «О персональных данных» и несет гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

|  |  |  |
| --- | --- | --- |
| **Начальник управления информатизации и коммуникаций** |  | **И.Н. Гвоздевский** |