

Приложение № 4 к приказу
от 28.06.2019 № 01-09/315
УТВЕРЖДЕНО

приказом генерального директора
КГБОУ ХКЦВР Созвездие
от 28.06.2019 № 01-09/315

РУКОВОДСТВО

администратора безопасности

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее руководство определяет обязанности, права и ответственность ответственного за защиту информации (администратора безопасности) краевого государственного бюджетного образовательного учреждения «Хабаровский краевой центр внешкольной работы «Созвездие» (далее – учреждение).

2. ОБЯЗАННОСТИ

2.1. Администратор безопасности обязан знать и выполнять требования законодательства Российской Федерации и локальных нормативных актов учреждения, устанавливающих правила обработки и защиты информации, в том числе персональных данных (далее – ПДн).

2.2. С целью защиты информации администратор безопасности обязан:

2.2.1. Выполнять и принимать меры для выполнения требований организационно-распорядительной документации по организации обработки и защиты информации.

2.2.2. Знать и выполнять требования внутреннего регламента учреждения.

2.2.3. Осуществлять установку, настройку и сопровождение технических средств защиты для ПДн.

2.2.4. Участвовать в контрольных и тестовых испытаниях и проверках организации защиты ПДн.

2.2.5. Участвовать в приемке новых программных средств.

2.2.6. Обеспечить доступ к защищаемой информации пользователям, для осуществления ими трудовых обязанностей.

2.2.7. Уточнять в установленном порядке обязанности пользователей по обработке информации.

2.2.8. Вести контроль над процессом осуществления резервного копирования информации.

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

2.2.10. Контролировать физическую сохранность технических средств и средств защиты информации (далее – СЗИ).

2.2.11. Контролировать исполнение пользователями введенного режима безопасности, а также правильность работы с СЗИ.

2.2.12. Контролировать исполнение пользователями правил пользования паролями.

2.2.13. Не допускать к работе на средствах вычислительной техники посторонних лиц.

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

2.2.15. В случае отказа работоспособности технических средств и программного обеспечения, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

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

3. ПРАВА

3.1. Привлекать к работам, связанным с обеспечением безопасности информации, сотрудников отдела информационных технологий.

3.2. Требовать от пользователей соблюдение и выполнение требований инструкций в соответствии с организационно-распорядительной документацией по защите информации.

3.3. Требовать от руководства организационного и материального обеспечения для безусловного выполнения своих обязанностей.

4. ОТВЕТСТВЕННОСТЬ

На администратора безопасности возлагается персональная ответственность:

4.1. за соблюдение режима конфиденциальности информации;

4.2. за правильность понимания и полноту выполнения задач, функций, прав и обязанностей возложенных на него;

4.3. за соблюдение требований локальных актов по вопросам обработки и защиты информации.