бюджетное учреждение профессионального образования Ханты-Мансийского автономного округа - Югры «Няганский технологический колледж»
(БУ «Няганский технологический колледж»)

П Р И К А З

«9» 09 2017 г. № 270

Нягань

Об утверждении инструкции
администратора информационных систем персональных данных

Во исполнение Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Инструкцию администратора информационных систем персональных данных БУ «Няганский технологический колледж» (далее – Инструкция).
2. Администратору информационных систем персональных данных в рамках своей деятельности руководствоваться прилагаемой Инструкцией.
3. Требования настоящего приказа довести до администратора информационных систем персональных данных.
4. Контроль за исполнением настоящего приказа оставляю.

И.о. директора О. В. Перминова

Приложение № 1 к приказу
от «08» сентября 2017 г. № 270

ИНСТРУКЦИЯ
администратора информационных систем персональных данных БУ «Няганский технологический колледж»

1. Общие положения

1.1 Настоящая инструкция определяет функциональные обязанности, ответственность и права администратора информационных систем персональных данных БУ «Няганский технологический колледж» (далее по тексту – Администратор).

1.2 Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3 Доступ к информационной системе администратор получает у ответственного за обеспечение безопасности персональных данных в информационных системах.

1.4 На время отсутствия (болезнь, отпуск, пр.) администратора его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

1.5 Администратор в своей работе руководствуется настоящей инструкцией.

1.6 Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности сведений конфиденциального характера, и не исключает обязательного выполнения их требований.

2. Функциональные обязанности

2.1 Администратор управляет конфигурацией информационной системы:

- поддерживает конфигурацию информационной системы (структуру информационной системы, состава, мест установки и параметров программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на информационную систему;
- осуществляет изменения конфигурации информационной системы, после согласования с ответственным обеспечение безопасности персональных данных в информационных системах;
- осуществляет изменения параметров настройки программного обеспечения и технических средств информационной системы, после согласования с ответственным обеспечение безопасности персональных данных в информационных системах;
- производит обновления программного обеспечения информационной системы, после согласования с ответственным за обеспечение безопасности персональных данных в информационных системах;
- восстанавливает работоспособность программного обеспечения и технических средств информационной системы;
- обеспечивает доступность и целостность программного обеспечения и технических средств;
- поддерживает установленные правила разграничения доступа в информационной системе;
- осуществляет наблюдение за состоянием системы.

2.2 Администратор выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее по тексту - инциденты), и реагирует на них:

- обнаруживает и идентифицирует инциденты, в том числе:
  - отказы в обслуживании,
  - сбои (перезагрузки) в работе средств защиты информации,

- нарушения правил разграничения доступа,
- неправомерные действия по сбору информации,
- иные события, приводящие к возникновению инцидентов;

– своевременно информирует ответственного за обеспечение безопасности персональных данных в информационных системах, о возникновении инцидентов информации в информационной системе;
– анализирует инциденты, в том числе определяет источники и причины возникновения инцидентов, а также оценивает их последствия;
– совместно с ответственным обеспечение безопасности персональных данных в информационных системах принимает меры по предотвращению повторного возникновения инцидентов.

2.3 Администратор выявляет ведет учет пользователей информационных систем персональных данных.

3. Права

3.1 Администратор имеет право:

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты персональных данных, несанкционированного доступа к персональным данным, утраты и/или порчи персональных данных и технических средств, входящих в состав информационной системы;
– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа к персональным данным в информационной системе;
– подавать свои предложения по совершенствованию организационных и технических мер по защите персональных данных.

4 Ответственность

4.1 Администратор информационной системы обязан:

– знать и выполнять требования настоящей инструкции, а также действующих нормативных и руководящих документов регламентирующих порядок действий по защите информации;
– выполнять на автоматизированном рабочем месте только те процедуры, которые требуются для выполнения его должностных обязанностей;
– соблюдать установленные правила разграничения доступа;
– покидая свое рабочее место на кратковременный срок блокировать доступ к операционной среде автоматизированного рабочего места.

4.2 Администратору информационной системы категорически запрещается:

– разглашать сведения ограниченного доступа, ставшие известными ему по роду работы;
– использовать неучтенные внешние машинные носители информации;
– подключать к автоматизированному рабочему месту мобильные устройства;
– самостоятельно устанавливать или модифицировать программное и (или) аппаратное обеспечение информационной системы;
– использовать компоненты программного и аппаратного обеспечения информационной системы в неслужебных (личных) целях;
– оставлять автоматизированное рабочее место без присмотра, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инцидентам информационной безопасности.

4.3 На администратора возлагается персональная ответственность за качество проводимых им работ по обеспечению бесперебойного и стабильного функционирования информационной системы.

4.4 Администратор несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными ему по роду работы.