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

П Р И К А З

«09» 09 2017 г. № 297

Нягань

Об утверждении инструкции ответственного за обеспечение безопасности персональных данных в информационных системах

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 ответственного за обеспечение безопасности персональных данных в информационных системах БУ «Няганский технологический колледж» (далее – Инструкция).
2. Ответственному за обеспечение безопасности персональных данных в информационных системах в рамках своей деятельности руководствоваться прилагаемой Инструкцией.
3. Требования настоящего приказа довести до ответственного за обеспечение безопасности персональных данных в информационных системах.
4. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. директора О. В. Перминова

Приложение № 1 к приказу
от «09» 09 2017 г. № 297

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах БУ «Няганский технологический колледж»

1. Общие положения

1.1 Настоящая инструкция определяет функциональные обязанности, ответственность и права ответственного за обеспечение безопасности персональных данных в информационных системах БУ «Няганский технологический колледж» (далее – Ответственный).

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

1.3 Ответственный назначается приказом директором.

1.4 На время отсутствия (болезнь, отпуск, пр.) ответственного его обязанности за осуществлением организационных и технических мероприятий по защите персональных данных в информационных системах, возлагаются на работника, назначенного и допущенного в установленном порядке.

1.5 Ответственный 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 Ответственный управляет системой защиты персональных данных в информационной системе:

- управляет доступом пользователей в информационную систему;
- управляет полномочиями пользователей в информационной системе;
- поддерживает установленные правила разграничения доступа в информационной системе;
- управляет средствами защиты информации, в том числе параметрами настройки программного обеспечения средств защиты информации;
- восстанавливает работоспособность средств защиты информации;
- устанавливает обновления программного обеспечения средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;
- осуществляет централизованное управление системой защиты персональных данных;
- информирует пользователей информационной системы об угрозах безопасности персональных данных;
- информирует пользователей информационной системы о правилах эксплуатации средств защиты информации;
- сопровождает функционирование системы защиты персональных данных в ходе эксплуатации информационной системы, включая корректировку эксплуатационной документации;
- поддерживает конфигурацию системы защиты персональных данных (структуру системы защиты персональных данных, состава, мест установки и параметров настройки средств защиты информации) в соответствии с эксплуатационной документацией на систему защиты персональных данных;
- управляет изменениями конфигурации системы защиты персональных данных, в том числе:
  - определяет типы возможных изменений,

- разрешает или отказывает во внесении изменений,
- документирует действия по внесению изменений,
- хранит данные об изменениях.

2.2 Ответственный 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;
- управляет изменениями конфигурации информационной системы, в том числе:
  - определяет типы возможных изменений,
  - разрешает или отказывает во внесении изменений,
  - документирует действия по внесению изменений,
  - хранит данные об изменениях;
- управляет параметрами настройки программного обеспечения и технических средств информационной системы;
- управляет обновлениями программного обеспечения информационной системы;
- восстанавливает работоспособность программного обеспечения и технических средств информационной системы;
- обеспечивает доступность и целостность программного обеспечения и технических средств;
- осуществляет наблюдение за состоянием системы.

2.3 Ответственный 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;
- анализирует инциденты, в том числе определяет источники и причины возникновения инцидентов, а также оценивает их последствия;
- планирует меры по устранению инцидентов, в том числе:
  - по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев,
  - устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирует и принимает меры по предотвращению повторного возникновения инцидентов.

2.4 Ответственный контролирует обеспечение уровня защищенности персональных данных, обрабатываемых в информационной системе:

- контролирует события безопасности и действия пользователей в информационной системе;
- контролирует (анализирует) защищенность персональных данных;
- анализирует и оценивает функционирование системы защиты персональных данных информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты персональных;

- документирует процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности персональных данных, обрабатываемых в информационной системе;
- принимает решения по результатам контроля (мониторинга) за обеспечением уровня защищенности персональных данных о доработке (модернизации) системы защиты персональных данных.

2.5 Ответственный ведет учет:

- ведет учет используемых средств защиты информации в информационных системах персональных данных;
- ведет учет используемых шифровальных (криптографических) средств защиты информации в информационных системах персональных данных, эксплуатационной и технической документации к ним;
- ведет учет съемных машинных носителей персональных данных (при их наличии).

2.6 Обеспечивает защиту персональных данных при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки персональных данных:

- обеспечивает архивирование персональных данных, содержащихся в информационной системе (архивирование должно осуществляться при необходимости дальнейшего использования персональных данных);
- обеспечивает уничтожение (стирание) персональных данных и остаточной информации с машинных носителей персональных данных, при необходимости передачи машинного носителя персональных данных в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;
- при выводе из эксплуатации машинных носителей данных, на которых осуществлялись хранение и обработка персональных данных, осуществляет физическое уничтожение этих съемных машинных носителей данных.

2.7 Осуществляет регулярный мониторинг включения БУ «Няганский технологический колледж» в ежегодный сводный план проведения плановых проверок на предмет соблюдения обязательных требований в сфере обработки персональных данных.

3 Права

3.1 Ответственный имеет право:

- требовать от работников – пользователей информационной системы соблюдения установленной технологии обработки персональных данных и выполнения организационно-распорядительной документации по обеспечению безопасности персональных данных;
- 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 информационных систем персональных данных;
- требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа к персональным данным;
- подавать свои предложения по совершенствованию организационных и технических мер по защите персональных данных.

4 Ответственность

4.1 Сотрудник, ответственный обеспечение безопасности персональных данных в информационных системах 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;
- покидая свое рабочее место на кратковременный срок блокировать доступ к операционной среде автоматизированного рабочего места.

4.2 Сотруднику, ответственному за обеспечение безопасности персональных данных в информационных системах 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;
- 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 сотрудника, ответственного за обеспечение безопасности персональных данных в информационных системах, возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты персональных данных.

4.4 Сотрудник, ответственный за обеспечение безопасности персональных данных в информационных системах, несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными ему по роду работы.