УТВЕРЖДАЮ
Директор СНТ (филиал)
ФГБОУ ВО "ЮГУ"
_____ И.С. Саркисян
"27" 12 2016г.

Инструкция

по проведению инструктажа по информационной безопасности

И-01-2016 Версия №1

Изм.№	Изм.№

ВВЕДЕНО В ДЕЙСТВИЕ
Приказом директора СНТ (филиал) ФГБОУ ВО ЮГУ
№ 242 от 27.12.2016г. 20 16г.

г.Сургут

Минобрнауки России Федеральное государственное бюджетное образовательное учреждение высшего образования «Югорский государственный университет» Сургутский нефтяной техникум (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет» (СНТ (филиал) ФГБОУ ВО «ЮГУ»)	СНТ (филиал) ФГБО ВО «ЮГУ»
Инструкция по проведению инструктажа по Информационной безопасности	Версия №1

ИНСТРУКЦИЮ РАЗРАБОТАЛ:

Инженер-электроник _____ 27.12.16 А.В.Горнов.
(подпись) (дд.мм.гг.)

СОГЛАСОВАНО:

Инженер по комплексной безопасности _____ 27.12.16. Ю.А. Ивакин.
(подпись) (дд.мм.гг.)

Юрисконсульт _____ 27.12.16. А.Р.Ахунова.
(подпись) (дд.мм.гг.)

Общие требования безопасности

1.1. Настоящая инструкция разработана с целью:

- сформулировать меры по информационной безопасности для работников техникума, соблюдение которых обеспечит безопасность персональных данных и иной конфиденциальной информации;
- обучить работников мерам информационной безопасности.

1.2. Настоящая инструкция распространяется на работников, работающих с персональными данными и иной конфиденциальной информацией техникума.

1.3. Инструктаж по информационной безопасности проводится инженером-электроником или инженером по комплексной безопасности техникума, согласно утвержденного Перечня должностных лиц техникума, на которых возложены обязанности по проведению инструктажа по информационной безопасности.

1.4. При инструктаже до инструктируемого должны быть доведены элементарные и базовые представления о мерах информационной безопасности.

1.5. Инструктаж завершается проверкой (путем устного опроса) усвоения работником мер информационной безопасности.

1.6. Перечень должностей и профессий работников техникума, которые должны проходить инструктаж по информационной безопасности утверждается директором техникума.

1.7. Термины, используемые в настоящей инструкции:

персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

субъект персональных данных - физические лица, которые вступили или изъявили желание вступить в правоотношения с Университетом;

документы, содержащие персональные данные - зафиксированная на материальном носителе идентифицируемая информация, созданная, полученная, сохраняемая в качестве доказательства при подтверждении правовых обязательств или деловой деятельности и содержащая персональные данные;

конфиденциальность персональных данных - обязательное для соблюдения техникумом или иными получившим доступ к персональным данным лицам, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

информационная система персональных данных (ИСПДн) — информационная система, представляющая собой совокупность персональных данных, а также

информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

ответственный за информационный ресурс - лицо, которое проектирует, разрабатывает, тестирует информационный ресурс, а также несет ответственность за техническое состояние ресурса;

учетная запись - хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам;

антивирусная защита - защита, которая включает в себя целый набор средств для предотвращения вредоносных действий различного характера;

автоматизированное рабочее место (АРМ) - индивидуальный комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий подготовку, редактирование, поиск и выдачу на экран, печать необходимых ему документов и данных;

несанкционированный доступ (НСД) - доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

2. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей

2.1. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные, разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

2.2. Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

2.3. Вход пользователя в систему осуществляется по выдаваемому ему имени учетной записи и персональному паролю.

2.4. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты, описанной в главе 8 настоящей инструкции.

2.5. Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;
- хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме, описанной в главе 7 настоящей инструкции;
- немедленно известить инженера-электроника при обнаружении:
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
- непредусмотренных отводов кабелей и подключенных устройств;

2.6. Пользователю АРМ категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

- считывать, записывать и хранить информацию на неучтенных машинных носителях информации (гибких магнитных дисках, флэш- накопителях и т.п.);
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или в ином месте машинные носители и распечатки, содержащие персональные данные;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;
- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные, а также размещать средства устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

2.7. В случае необходимости добавления в группу локальных администраторов на АРМ пользователю необходимо написать служебную записку на имя директора Сургутского нефтяного техникума согласно форме Приложения 2.

2.8. При обнаружении каких-либо нарушений требований информационной безопасности немедленно сообщить об этом своему непосредственному или прямому руководителю, который обязан принять меры по устранению нарушений.

3. Предоставление доступа работникам к информационным ресурсам, содержащим персональные данные

3.1. Перечень информационных систем, в которых разрешено обрабатывать персональные данные, и список лиц ответственных лиц за каждый информационный ресурс, содержащий персональные данные, утверждаются приказом директора.

3.2. Для предоставления доступа к информационным ресурсам для работника или для выгрузки единовременного отчета с персональными данными, руководителю его структурного подразделения необходимо написать служебную записку на имя ответственного лица за организацию обработки персональных данных. В служебной записке обосновывается необходимость допуска сотрудника к персональным данным, состав персональных данных, необходимые права по обработке персональных данных, срок, на который предоставляется допуск сотрудника к обработке персональных данных.

3.3. Прекращение доступа работнику осуществляется на основании служебной записки начальника структурного подразделения инженеру-электронику.

Основанием для прекращения доступа является:

- изменение должности или подразделения сотрудника;
- уход в длительный отпуск (например, отпуск по беременности и родам, по уходу за ребенком и пр.);
- увольнение работника.

3.4. Для предоставления или ограничения доступа к информационным ресурсам, содержащим персональные данные определяется порядок работы, описанный в приложении 1.

3.5. Для предоставления доступа необходимо инженеру-электронику внести работника в журнал учета работников, допущенных к работе с персональными данными.

4. Инструкция по обработке персональных данных без использования средств автоматизации.

4.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

4.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

4.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

4.4. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

4.5. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.6. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

5. Правила работы с обезличенными данными

5.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных техникума и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. Для обезличивания персональных данных создается экспертная комиссия в составе не менее 3 человек, после которой составляется акт. Ответственность за обезличивание персональных данных несет инженер-электроник.

5.3. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение - понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт);
- деление сведений на части и обработка в разных информационных системах;
- иные способы.

5.4. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

5.5. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

5.6. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение инструкций по организации парольной и антивирусной защите (главы 7-8 настоящей инструкции).

5.7. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

6. Инструкция по организации парольной защиты

6.1. Личные пароли генерируются и распределяются централизованно инженером-электроником, техником:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать одна заглавная буква и одна цифра;
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), а также легко подбираемые пароли (Qwel23, Qazl23, Asdl23 и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам;

6.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 месяцев.

6.2. Внеплановая смена личного пароля, закрытие или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, отпуск по уходу за ребенком и т.п.) должна производиться инженером–электроником немедленно после окончания последнего сеанса работы данного пользователя с системой.

6.3. В случае компрометации (утеря, передача другому лицу) личного пароля, пользователь ИСПДн обязан незамедлительно сообщить об этом начальнику отдела информационной безопасности для принятия соответствующих мер.

6.4. При смене работником фамилии, имя учетной записи подлежит изменению. Изменение имени учетной записи осуществляется работниками учебно-производственного центра информационных технологий.

7. Инструкция по организации антивирусной защиты

7.1 К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

7.2. Установка и настройка средств антивирусного контроля осуществляется инженером-электроником, техником.

7.3 При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестре операционной системы.

7.4. Полному антивирусному контролю автоматизированные рабочие места должны подвергаться не реже одного раза в две недели.

7.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.).

7.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения инженер-электроник должен выполнить антивирусную проверку на защищаемых серверах и пользовательских АРМ.

7.7. При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с техником должен провести внеочередной антивирусный контроль своего АРМ.

7.8. В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и инженера-электроника, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

7.9. Не открывать незнакомые файлы с электронной почты, USB- носителей и т.п.

8. Ответственность работников за невыполнение настоящей инструкции

8.1. Работники, допустившие невыполнение настоящей инструкции, в зависимости от последствий ее невыполнения, привлекаются к дисциплинарной, административной, уголовной или гражданской ответственности.

8.2. Ответственность за организацию антивирусного контроля, организацию парольной защиты и соблюдение требований настоящей инструкции возлагается на инженера-электроника, инженера по комплексной безопасности, техника.

8.3. Ответственность за соблюдение требований настоящей инструкции возлагается на работников, непосредственно работающих на АРМ, и руководителей их структурных подразделений.

8.4. Периодический контроль над общим состоянием антивирусной защиты, контроль за выполнением требований парольной защиты, предоставлением и ограничением доступа работникам техникума к информационным ресурсам, а также выполнением требований настоящей инструкции работниками СНТ (филиал) ФГБУ ВО «ЮГУ» осуществляется инженером-электроником, инженером по комплексной безопасности.

9. Заключительные положения

9.1. Вопросы, не рассмотренные настоящей инструкцией, регулируются в соответствии с действующим законодательством Российской Федераций.

9.2. Все работники техникума должны быть ознакомлены под роспись с данной инструкцией и изменениями к ней.

Приложение 1

Порядок работы по предоставлению или ограничению доступа к ИСПДн

№ п/п	Действие	Срок	Ответственное лицо
Прием работника на работу / Предоставление доступа			
1	Написание служебной записки на имя директора техникума	По мере необходимости	Руководитель структурного подразделения
2	Согласование служебной записки.	В течение двух рабочих дней	Директор техникума
3	Ознакомление под роспись работника с перечнем доступных информационных ресурсов, внесение работника в журнал учета работников, допущенных к работе с конфиденциальной информацией.	В течение одного рабочего дня	Инженер-электроник
4	Предоставление доступа к необходимым информационным ресурсам ФГБОУ ВО «ЮГУ», СНТ (филиал ФГБОУ ВО «ЮГУ»)	В течение одного рабочего дня	Инженер-электроник
Перевод работника в другое подразделение/на другую должность			
1	Написание служебной записки на имя директора техникума	По мере необходимости	Руководитель текущего структурного подразделения
2	Согласование служебной записки. Передача ее инженеру-электронику	В течение двух рабочих дней	Директор техникума
3	Внесение изменений в журнал учета работников, допущенных к работе с персональными данными.	В течение одного рабочего дня	Инженер-электроник

4	Изменение доступа в корпоративную информационную среду СНТ (филиал ФГБОУ ВО «ЮГУ»)	В течение одного рабочего дня	Инженер-электроник
Увольнение работника из ФГБОУ ВО «ЮГУ»			
1	Передача копии приказа об увольнении работника инженеру-электронику	В течение двух рабочих дней после подписания приказа	Специалист по персоналу
2	Внесение изменений в журнал учета работников, допущенных к работе с персональными данными. Ограничение доступа в корпоративную среду СНТ (филиал ФГБОУ ВО «ЮГУ»)	В течение двух рабочих дней после подписания приказа	Инженер-электроник

Приложение 2

Форма служебной записки для добавления в группу локальных администраторов на компьютер

Директору СНТ (филиал) ФГБОУ ВО «ЮГУ»
Саркисян И.С.
От_____
_____

Служебная записка

В связи с _____
прошу добавить в группу локальных администраторов на компьютер (АРМ) каб. № ___ инвентарный номер: _____ ;

Обязуюсь:

1) Не использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

2) Самовольно не вносить какие-либо изменения в конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

3) Не оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры).

Подтверждаю, что предупрежден об ответственности за нарушение вышеизложенных правил, а также локальных нормативных актов, принятых в СНТ (филиал) ФГБОУ ВО «Югорский государственный университет» в сфере информационной безопасности.

_____ _____ .

_____ _____
_____

(дата) подпись (расшифровка)

Согласовано:

Инженер-электроник _____/ Горнов А.В./