Директор С.С. Лузан

Описание технологического процесса обработки информации в информационных системах персональных данных ГБПОУ НСО «Новосибирский профессионально-педагогический колледж»

1. Назначение и цели создания ИСПДн

Назначение информационных систем персональных данных (далее - ИСПДн) «Студенты» и «Бухгалтерия и кадры» Государственного бюджетного профессионального образовательного учреждения Новосибирской области «Новосибирский профессионально-педагогический колледж» (далее - ГБПОУ НСО «Новосибирский профессионально-педагогический колледж»): сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание информации, необходимой для достижения целей обработки конфиденциальной информации.

Цели ИСПДн «Студенты» - ведение образовательной деятельности по начальному профессиональному образованию, профессиональной подготовке и дополнительному образованию, согласно лицензии.

Цель ИСПДн «Бухгалтерия и кадры» - ведение бухгалтерского и кадрового учета.

2. Расположение ИСПДн

Технические средства ИСПДн «Студенты» и ИСПДн «Бухгалтерия и кадры» располагаются по адресу: 630048, г. Новосибирск, ул. Немировича-Данченко, д. 121.

3. Используемые программные средства

Разрешенное к использованию программное обеспечение указывается в отдельном перечне, который разрабатывается ответственным за обеспечение безопасности персональных данных.

Функции, права и обязанности ответственного за обеспечение безопасности персональных данных регламентируются специально разработанной инструкцией, утверждаемой директором ГБПОУ НСО «Новосибирский профессионально-педагогический колледж».

4. Источники данных

Источниками данных для ИСПДн являются:

— сведения, вводимые с клавиатуры;

— конфиденциальная информация (файлы) на отчуждаемых МНИ, поступившая из сторонних организаций;

— конфиденциальная информация (файлы), поступившая по защищенным каналам связи;

— персональные данные.

5. Доступ к информационным ресурсам

5.1 Общая часть

Права доступа к информационным ресурсам назначаются каждому пользователю ИСПДн на основании разрешительной системы доступа, разрабатываемой ответственным за обеспечение безопасности персональных данных.

Вход в систему осуществляется по уникальному паролю конкретного пользователя ИСПДн (не менее 6 символов). При успешном входе в систему пользователь получает права доступа к устройствам, каталогам, файлам и программам, установленным ответственным за обеспечение безопасности персональных данных.

При увольнении пользователя ИСПДн или переходе в другое подразделение ответственным за обеспечение безопасности персональных данных на основании приказа в последний день работы пользователя (или иной день, указанный в приказе), производится удаление учетной записи пользователя и всех его ресурсов (за исключением необходимых для работы других пользователей).

5.2 Начало сеанса работы

Перед началом сеанса работы пользователь включает ПЭВМ и проходит процедуру аутентификации.

В процессе аутентификации пользователь использует свой личный пароль. Смена личного пароля производится не реже 1 раза в 3 месяца. Контроль данного процесса осуществляется ответственным за обеспечение безопасности персональных данных.

5.3 Регистрация пользователей и назначение прав доступа

Регистрация пользователей и назначение прав доступа производится ответственным за обеспечение безопасности персональных данных. Пользователями ИСПДн являются сотрудники ГБПОУ НС О «Новосибирский профессионально-педагогический колледж».

Зарегистрированный пользователь ИСПДн устанавливает свой личный пароль.

Права доступа устанавливаются пользователю средствами ОС в соответствии с разрешительной системой доступа, разработанной ответственным за обеспечение безопасности персональных данных.

Удаление пользователя выполняется однократно при необходимости выведения сотрудника из числа пользователей ИСПДн.

5.4 Работа с файлами документов, внесение изменений, хранение, передача

Файлы документов разрабатываются на рабочем месте пользователем. Работа пользователя при подготовке файла документа возможна только после успешного прохождения процедуры аутентификации.

Пользователи имеют право постоянного хранения файлов с конфиденциальной и не конфиденциальной информацией на жестком магнитном диске только в специально выделенных ответственным за обеспечение безопасности персональных данных каталогах, указанных в Перечне защищаемых ресурсов.

По окончании сеанса подготовки документа производится его сохранение в виде файла в разрешенном ответственным за обеспечение безопасности персональных данных каталоге или на закрепленный за пользователем отчуждаемый носитель, соответствующим образом зарегистрированный.

В случае отсутствия необходимости дальнейшей работы с документом, впервые набранным с клавиатуры, пользователь может отказаться от сохранения его в виде файла. Также пользователь может отказаться от сохранения внесенных в файл изменений.

5.5 Уничтожение файлов, содержащих конфиденциальные данные

Удаление данных (файлов) и временных файлов производится штатными средствами ОС.

При установке ОС отключена функция удаления файлов через «корзину».

В случае установки СЗИ от НСД будет активирована функция затирания данных с применением не менее одного цикла затирания.

Запрещается удалять информацию с магнитных носителей иными программными средствами.

5.6 Работа с отчуждаемыми носителями

Для разработки и хранения файлов с конфиденциальными данными могут также использоваться отчуждаемые МНИ, учтенные в установленном порядке в соответствии с требованиями конфиденциального делопроизводства.

Отчуждаемые носители при необходимости выдаются каждому пользователю из числа сотрудников, обрабатывающих конфиденциальные сведения. Выданный носитель предназначен только для хранения файлов подготовленных документов. Операции с отчуждаемым носителем для конфиденциальной информации могут проводиться только на ПЭВМ, входящей в состав ИСПДн, аттестованных по требованиям информационной безопасности в соответствии руководящими документами ФСТЭК России России.

5.6.1 Подготовка отчуждаемого носителя пользователя. Выведение из обращения отчуждаемых носителей информации

При необходимости создания нового отчуждаемого носителя пользователь регистрирует его в соответствии с требованиями конфиденциального делопроизводства.

При необходимости пользователь сдает зарегистрированный отчуждаемый МНИ ответственному за обеспечение безопасности

персональных данных с целью его подготовки для дальнейшего использования на ПЭВМ, входящей в состав ИСПДн.

Выведение носителя из обращения производится путем его физического уничтожения, при этом составляется акт соответствующей формы.

5.6.2 Создание файлов на отчуждаемом носителе

Условиями, необходимыми для выполнения данной процедуры, являются:

- пользователю разрешено самостоятельно копировать файлы на отчуждаемый носитель и обратно;
- наличие у пользователя подготовленного и зарегистрированного соответствующим образом МНИ.

5.6.3 Хранение МНИ пользователя

Хранение МНИ пользователя должно осуществляться в соответствии с требованиями конфиденциального делопроизводства.

5.7 Резервное копирование

Резервное копирование информационных ресурсов производится ответственным за обеспечение безопасности персональных данных или пользователем в соответствии с правами доступа на МНИ, учтенным в установленном порядке в соответствии с требованиями конфиденциального делопроизводства.

5.8 Передача информации на отчуждаемых носителях

Передача файлов конфиденциальных документов на отчуждаемых носителях в другие организации, производится в соответствии с требованиями конфиденциального делопроизводства. Передача файлов конфиденциальных документов на отчуждаемых носителях в организации иной ведомственной подчинённости производится на основании совместно заключенных соглашений в соответствии с требованиями конфиденциального делопроизводства.

5.9 Завершение сеанса работы

По завершении работы пользователь выполняет штатную процедуру завершения работы в Windows, выключает рабочую станцию и сдаёт имеющиеся отчуждаемые носители сотруднику, ответственному за ведение конфиденциального делопроизводства, или помещает их в личный сейф.

Разработал

ответственный за обеспечение
безопасности персональных данных А.С. Кечкин