Частное профессиональное образовательное учреждение
«НИЖЕГОРОДСКИЙ БИЗНЕС-КОЛЛЕДЖ»
(ЧПОУ «НБК»)

УТВЕРЖДЕНА
приказом директор
от 28 августа 2015г.
№ 02-02/81

ПОЛИТИКА
в отношении обработки персональных данных при обработке в информационных системах в Частном профессиональном образовательном учреждении «Нижегородский бизнес-колледж»

Нижний Новгород
2015

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Настоящая Политика в отношении обработки персональных данных составлена в соответствии с ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и действует в отношении персональных данных, которые ЧПОУ «Нижегородский бизнес-колледж» (далее – колледж) может получить от субъектов персональных данных.

1.2.Основные понятия, используемые в Политике:

— персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

— обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.3.Обработка персональных данных в основана на следующих принципах:

— осуществления на законной и справедливой основе;

— соответствия целей обработки персональных данных полномочиям;

— соответствия содержания и объема обрабатываемых персональных данных целям обработки персональных данных;

— достоверности персональных данных, их актуальности и достаточности для целей обработки, недопустимости обработки избыточных по отношению к целям сбора персональных данных;

— ограничения обработки персональных данных при достижении конкретных и законных целей, запретом обработки персональных данных, несовместимых с целями сбора персональных данных;

— запрета объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

— осуществления хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

1.4.В соответствии с принципами обработки персональных данных определены цели обработки персональных данных:

— для исполнения условий трудового договора и осуществления прав и обязанностей в соответствии с законодательством;

— для принятия решений по обращениям граждан Российской Федерации в соответствии с законодательством.

1.5.Администрация колледжа обрабатывает персональные данные, которые может получить от следующих субъектов персональных данных:

— граждан, состоящих в отношениях, регулируемых трудовым законодательством.

— граждан, обучающихся в колледже.

1.6. Срок хранения персональных данных субъекта персональных данных определяется в соответствии с действующим законодательством и иными нормативными правовыми документами.

2.ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ПЕРЕДАЧИ ТРЕТЬИМ ЛИЦАМ

2.1.При обработке персональных данных колледж руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Положением об обработке и защите персональных данных, Положением о локальной вычислительной сети и Политикой.

2.2.Субъект персональных данных обладает правами, предусмотренными Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3. МЕРЫ, ПРИМЕНЯЕМЫЕ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1.Колледж принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных субъектов персональных данных.

К таким мерам, в частности, относятся:

— назначение сотрудника или сотрудников, ответственных за организацию обработки персональных данных;

— осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;

— ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями действующего законодательства о персональных данных, требованиями к защите персональных данных и иными документами по вопросам обработки персональных данных;

— определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

— применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

— установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;

— осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

— разработка локальных документов по вопросам обработки персональных данных.

ПРИЛОЖЕНИЕ 1

Обобщенная модель угроз для ЛИС II типа*

Исходный класс защищенности – средний.

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Звукоизоляция	
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Положения
2. Угрозы несанкционированного доступа к информации						
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн						
2.1.1. Кража ПЭВМ	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	
					Хранение в сейфе	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Положения
2.1.4. Кражи, модификации,	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	
					Решетки на окна	

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
уничтожения информации.					Металлическая дверь	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окнах	Охрана
					Металлическая дверь	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);						
2.2.1. Действия вредоносных программ (вирусов)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Технологический процесс обработки
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая	Средняя	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя
						Инструкция ответственного

Наименование угрозы обязанностей	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Низкая	Неактуальная		Инструкция пользователя
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угрозы выявления паролей по сети.	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности
2.5.2. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности
2.5.3. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя
2.5.4. Угрозы типа «Отказ в	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Технологический процесс Инструкция пользователя

Наименование угрозы обслуживании».	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
						Инструкция администратора безопасности
						Резервирование
2.5.5. Угрозы удаленного запуска приложений.	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
2.5.6. Угрозы внедрения по сети вредоносных программ.	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности

**- ЛИС II типа – локальная информационная система, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.*