

**Автономная некоммерческая организация профессионального обучения
«Колледж предпринимательских и цифровых технологий»
(АНО ПО «Колледж предпринимательских и цифровых технологий»)**

650000, г. Кемерово, ул. Н. Островского, д. 12, Тел. 89511607451
e-mail: zifra42@mail.ru; <https://zifra42.ru>
ОКПО 54572550; ОГРН 1204200005195; ИНН/КПП 4205388631/420501001

ПРИНЯТ

на Педагогическом совете
протокол № 3 от 25.10.2024 г.

УТВЕРЖДАЮ

Директор АНО ПО «Колледж
предпринимательских и цифровых
технологий»

О. М. Неведрова
Приказ № 62 от 01.11.2024

**ПОРЯДОК
оценки риска (вреда) субъектам персональных данных
АНО ПО «Колледж предпринимательских и цифровых технологий»**

Кемерово 2024

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение

Настоящий Порядок оценки возможного риска (вреда) субъектам персональных данных АНО ПО «Колледж предпринимательских и цифровых технологий» (далее –Порядок) определяет методику и порядок оценки вреда, который может быть причинён субъекту персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в АНО ПО «Колледж предпринимательских и цифровых технологий» (далее – Колледж).

1.2. Цель разработки Порядка

Настоящий Порядок принят в целях обеспечения соответствия процессов обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Область применения

Настоящий документ применяется:

- к процессам Колледжа, в которых ведется обработка персональных данных;
- ко всем сотрудникам, независимо от их местоположения.

1.4. Аудитория

Порядок предназначен для следующих категорий сотрудников Колледжа:

- сотрудник, ответственный за организацию обработки персональных данных;
- руководители, обрабатывающие персональные данные;
- лица, которым Колледжем поручено обрабатывать персональные данные.

Под сотрудниками в настоящем Порядке понимаются лица, состоящие в трудовых или договорных отношениях со Колледжем.

Перечисленные сотрудники перед предоставлением доступа к персональным данным должны быть ознакомлены с настоящим документом в соответствии с локальными нормативными актами.

1.5. Нормативные ссылки

Положение разработано в целях реализации требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.6. Срок действия и порядок внесения изменений

Порядок действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим.

Порядок подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, требований со стороны партнеров, изменения оценки рисков информационной безопасности.

Изменения в документ вносятся путем издания новой версии, утверждением его директором колледжа и ознакомления с ним сотрудников, а также лиц, осуществляющих обработку персональных данных.

После принятия Порядка (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

2. ОСНОВНЫЕ ПОНЯТИЯ

2.1. В настоящем Порядке используются основные понятия:

2.1.1. Информация - сведения (сообщения, данные) независимо от формы их представления;

2.1.2. Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

2.1.3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

2.1.4. Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;

2.1.5. Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

2.1.6. Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет

понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

2.1.7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;

2.1.8. Оценка возможного вреда - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. ОЦЕНКА ВОЗМОЖНОГО ВРЕДА СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Методика оценки возможного вреда субъекту персональных данных

3.1.1. Субъекту персональных данных может быть причинён вред в форме:

- убытков – расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

- морального вреда – физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.1.2. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.1.3. Оценка уровня вреда, который может быть причинен субъекту персональных данных в случае реализации угроз безопасности информации, проводится путем оценки тяжести последствий от нарушения каждого из свойств безопасности персональных данных в отдельности.

3.1.4. Вводятся три вербальных градаций показателя уровня вреда:

- вред отсутствует – если нарушение свойств безопасности персональных данных не может привести к каким-либо негативным последствиям для субъекта персональных данных;

- низкий уровень вреда – если нарушение свойств безопасности персональных данных может привести к незначительным негативным последствиям для субъекта персональных данных;

- средний уровень вреда – если нарушение свойств безопасности персональных данных может привести к негативным последствиям для субъекта персональных данных;

- высокий уровень вреда – если нарушение свойств безопасности персональных данных может привести к значительным негативным последствиям для субъекта персональных данных.

3.1.5. Порядок проведения оценки возможного вреда субъекту персональных данных. Оценка возможного вреда субъекту персональных данных осуществляется Комиссией по обеспечению безопасности персональных данных, в соответствии с методикой, описанной в разделе 2.1 настоящего Порядка.

3.1.6. По результатам оценки уровня возможного вреда субъекту персональных данных оформляется Протокол оценки возможного вреда субъекту персональных данных (далее – Протокол).

3.1.7. Допускается оформление одного Протокола на несколько категорий субъектов персональных данных.

3.1.8. Типовая форма Протокола приведена в Приложении 2.

3.1.9. Оценка возможного вреда подлежит пересмотру не реже 1 раза в год.

4. ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА, А ТАКЖЕ

СООТНЕСЕНИЯ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ КОЛЛЕДЖЕМ МЕР

4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным в АНО ПО «Колледж предпринимательских и цифровых технологий» за защиту информации, в соответствии с методикой, описанной в разделе 3 настоящего Порядка, и на основании экспертных значений, приведенных в Приложении 1.

ПРИЛОЖЕНИЕ 1

Оценка вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых Колледжем мер

N п/п	Требования Федерального закона "О персональных данных", которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
1	порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;	Убытки и моральный вред	+	средний	В соответствии с законодательством в области защиты информации и Положением по обеспечением безопасности персональных данных
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
2	порядок и условия применения средств защиты информации;	Убытки и моральный вред	+	средний	В соответствии с технической документацией на систему защиты АИСПД
		Целостность	+		
		Доступность			
		Конфиденциальность			
3	эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;	Убытки и моральный вред	+	высокий	Программа и методика испытаний систем защиты
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
4	состояние учета машинных носителей персональных данных;	Убытки и моральный вред			Инструкция по учету машинных носителей информации
		Целостность			
		Доступность			
		Конфиденциальность			
5	соблюдение правил доступа к персональным данным;	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
		Целостность	+		
		Доступность			
		Конфиденциальность	+		
6	наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;	Убытки и моральный вред	+	средний	Мониторинг средств защиты информации на наличие фактов доступа к ПД
		Целостность			
		Доступность			
		Конфиденциальность	+		
7	мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Убытки и моральный вред		низкий	Применение резервного копирования
		Целостность			
		Доступность	+		
		Конфиденциальность	+		
8	осуществление мероприятий по обеспечению целостности персональных данных.	Убытки и моральный вред		низкий	Организация режима доступа к техническим и программным средствам
		Целостность	+		
		Доступность			
		Конфиденциальность			

УТВЕРЖДАЮ
Директор АНО ПО «Колледж
предпринимательских и
цифровых технологий»
_____ О.М. Неведрова
« ____ » _____ 2024г.

ПРОТОКОЛ № _____
оценки возможного вреда субъектам персональных данных

« ____ » _____ 20 ____

1. Настоящий Протокол составлен Комиссией по обеспечению безопасности персональных данных АНО ПО «Колледж предпринимательских и цифровых технологий», назначенной приказом от « ____ » _____ 20 ____ г. № _____ в составе:

председатель комиссии: _____ / должность, ФИО

члены комиссии:

_____ / должность, ФИО

_____ / должность, ФИО

_____ / должность, ФИО

с целью оценки возможного вреда субъекту персональных данных.

2. В ходе проведения оценки возможного вреда субъектам персональных данных комиссия руководствовалась следующими документами:

– Порядок оценки возможного вреда субъектам персональных данных от « ____ » _____ 20 ____ г.;

– Политика в отношении обработки персональных данных « ____ » _____ 20 ____ г.

3. Результаты оценки возможного вреда субъектам персональных данных приведены в таблице 1.

Таблица 1 - Исходные данные для определения необходимого уровня защищенности

№ п/п	Категория субъектов	персональных данных	Нарушаемое свойство
1	Работники	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
2	Близкие родственники работников	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
3	Уволенные работники	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий

4	Кандидаты вакантных должностей на замещение	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
5	Обучающиеся	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
6	Родители (законные представители) обучающихся, родственники обучающихся	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
7	Дети и родители (законные представители) детей, поступающих в образовательную организацию	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
8	Лица, ранее обучавшиеся в образовательной организации	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
9	Физические лица - подрядчики по договорам гражданско-правового характера	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
10	Посетители колледжа	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
11	Представители контрагентов оператора (юридических лиц)	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний / Низкий/Высокий
		Доступность	Отсутствует/Средний / Низкий/Высокий
12	Физические лица – фигуранты публикаций, лица, изображенные на публикуемых фотографиях	Конфиденциальность	Отсутствует/Средний / Низкий/Высокий
		Целостность	Отсутствует/Средний /

			<i>Низкий/Высокий</i>
		Доступность	<i>Отсутствует/Средний / Низкий/Высокий</i>
13	Пользователь официального сайта колледжа в информационно-телекоммуникационной сети «Интернет», направивший обращение посредством форм обратной связи	Конфиденциальность	<i>Отсутствует/Средний / Низкий /Высокий</i>
		Целостность	<i>Отсутствует/Средний / Низкий/Высокий</i>
		Доступность	<i>Отсутствует/Средний / Низкий/Высокий</i>

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /