

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЮСТИЦИИ»
(ДГУЮ Минюста России)

П Р И К А З

01 апреля 2024г.

г. Донецк

№ 241

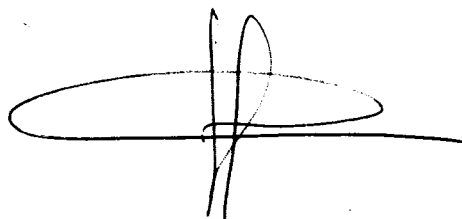
Об утверждении Положения о защите персональных данных обучающихся и работников федерального государственного бюджетного образовательного учреждения высшего образования «Донбасский государственный университет юстиции» (ДГУЮ Минюста России).

В соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных», в целях совершенствования обработки персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Донбасский государственный университет юстиции» (ДГУЮ Минюста России)),

приказываю:

1. Утвердить Положение о защите персональных данных обучающихся и работников федерального государственного бюджетного образовательного учреждения высшего образования «Донбасский государственный университет юстиции» (ДГУЮ Минюста России) (далее – Положение) в соответствии с приложением.
2. Начальнику управления делами Лыгину Р.А. обеспечить размещение Положения на сайте ДГУЮ Минюста России.
3. Начальнику отдела канцелярии и архива Копер Е.А. довести настоящий приказ до сведения всех работников ДГУЮ Минюста России.
4. Контроль за исполнением настоящего приказа возложить на начальника организационно-правового управления Кашпер А.А.

Ректор



Н.А. Нарыжный

Положение
о защите персональных данных обучающихся и работников федерального
государственного бюджетного образовательного учреждения высшего образования
«Донбасский государственный университет юстиции»
(ДГУЮ Минюста России).

1. Общие положения

1.1. Положение о защите персональных данных обучающихся и работников (далее - Субъектов) федерального государственного бюджетного образовательного учреждения высшего образования «Донбасский государственный университет юстиции» (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 01.11.2012 № 1119, которым утверждены правила защиты персональных данных, приказом ФСТЭК РФ от 18.02.2013 № 21 с перечнем мер по обеспечению безопасности данных при их обработке, а также Трудовым кодексом Российской Федерации.

1.2. Положение действует в отношении всех персональных данных, которые обрабатываются в федеральном государственном бюджетном образовательном учреждении высшего образования «Донбасский государственный университет юстиции» (далее - ДГУЮ Минюста России, оператор).

1.3. Настоящее Положение вступает в силу с момента его утверждения приказом ректора ДГУЮ Минюста России.

1.4. Положение подлежит пересмотру в случае изменения законодательства Российской Федерации в сфере персональных данных.

1.5. Настоящее Положение публикуется в свободном доступе в информационно-телекоммуникационной сети «Интернет» на официальном сайте ДГУЮ Минюста России.

2. Защита персональных данных

2.1. Оператор принимает следующие меры по защите персональных данных:

- назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных;
- разработка политики в отношении обработки персональных данных;

- установление правил доступа к персональным данным, обеспечение регистрации и учета всех действий, совершаемых с персональными данными;
- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;
- обнаружение фактов несанкционированного доступа к персональным данным;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников, непосредственно осуществляющих обработку персональных данных положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Оператора в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
- определение типа угроз безопасности и уровней защищенности персональных данных, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

2.3. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

2.4. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

2.5. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

2.6 Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

2.7. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

2.8. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

2.9 Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

2.10. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах

персональных данных», необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

2.11. В целях защиты персональных данных на бумажных носителях Оператор:

- приказом назначает ответственного за обработку персональных данных;
- ограничивает допуск в помещения, где хранятся документы, которые содержат персональных данных работников;
- хранит документы, содержащие персональные данные работников и обучающихся в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

2.12. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, управления бухгалтерского учета, планово-экономической работы и финансового контроля и отдела охраны труда и гражданской обороны.

2.13. Работники отдела кадров, управления бухгалтерского учета, планово-экономической работы и финансового контроля и отдела охраны труда и гражданской обороны, допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных.

2.14. Допуск к документам, содержащим персональные данные работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.

2.15. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.16. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.