

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

№ 242

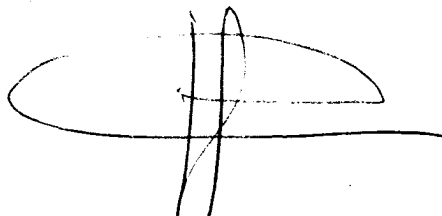
Об утверждении Положения о порядке действий в случае утечки персональных данных обучающихся и работников федерального государственного бюджетного образовательного учреждения высшего образования «Донбасский государственный университет юстиции» (ДГУЮ Минюста России).

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 порядке действий в случае утечки 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 порядке действий в случае утечки 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 порядке действий в случае утечки 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. УВЕДОМЛЕНИЕ В РОСКОНАДЗОР И ВНУТРЕННЕЕ РАССЛЕДОВАНИЕ В
СЛУЧАЕ УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И
ОБУЧАЮЩИХСЯ**

2.1. Обнаружив факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан в течение 24 часов сообщить в Роскомнадзор о

произошедшем инциденте и о его предполагаемых причинах, о вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с Роскомнадзором по вопросам, связанным с выявленным инцидентом.

2.2. Сообщение передаётся через Портал персональных данных, на котором Роскомнадзор организовал соответствующий сервис в разделе «Инциденты (утечки)» на странице «Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных».

2.3. Для обеспечения необходимого уровня защищенности в ДГУЮ Минюста России организованы:

- режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечена сохранность носителей персональных данных;

- утвержден документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- используются средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- установлены сертифицированные средства защиты информации, включая антивирусное ПО;

- назначено должностное лицо, ответственное за обеспечение безопасности персональных данных в информационной системе.

2.4. ДГУЮ Минюста России может воспользоваться услугами сторонних квалифицированных организаций и специалистов. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет именно оператор.

2.5. Если оператор персональных данных принял все необходимые и достаточные меры для обеспечения безопасности персональных данных в соответствии с требованиями законодательства Российской Федерации, но, несмотря на это, произошел инцидент, повлекший за собой нарушение прав субъектов персональных данных, состав правонарушения в действиях оператора отсутствует. В таком случае в уведомлении указываются причины, повлекшие нарушение прав субъектов персональных данных, которые оператор не мог контролировать. Характеризуя персональные данные, пострадавшие в ходе инцидента, приводится в уведомлении информация о содержании скомпрометированной базы данных (категории субъектов персональных данных (например, работники, обучающиеся, и др.), примерное количество записей, перечень категорий персональных данных (например, ФИО, дата рождения, данные документа, удостоверяющего личность, сведения об образовании и др.), актуальность базы данных, а также период, в течение которого собраны данные.

2.6. В уведомлении должны быть указаны принятые меры по устранению

последствий инцидента. К ним относятся:

- восстановление функциональности системы защиты персональных данных;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

После уведомления об инциденте в течение 24 часов с момента его выявления, в течение 72 часов необходимо проинформировать Роскомнадзор о результатах внутреннего расследования происшествия, а также предоставить сведения о виновниках (при наличии).

2.7. Во втором уведомлении указывается итоговая информация о результатах внутреннего расследования, в том числе: о причинах, повлекших неправомерное распространение персональных данных; о нанесенном правам субъекта персональных данных вреде; об информационной системе, к которой был осуществлен несанкционированный доступ; о лицах, чьи действия стали причиной инцидента (ФИО и должность сотрудника оператора или ФИО, наименование, IP-адрес, предполагаемое местонахождение стороннего виновника, если эту информацию удалось установить); о дополнительных мерах, принятых по результатам внутреннего расследования (по устранению доступа, недопущению подобных инцидентов в будущем и иные); о решении оператора с указанием его реквизитов о проведении внутренней проверки.

2.8. Если системы оператора подверглись хакерской атаке, он, помимо уведомления Роскомнадзора, обязан передать сведения о взломе, повлекшем неправомерную передачу (предоставление, распространение, доступ) персональных данных, в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами. Кроме того, они привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

Руководители структурных подразделений, в которых происходит обработка персональных данных, несут персональную ответственность за обеспечение защиты обрабатываемых и хранящихся в их подразделениях персональных данных Субъектов персональных данных.