МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный университет»
(Астраханский государственный университет)

ПРИКАЗ

28.08.2015 № 01-01/742

Об утверждении инструкции о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

Во исполнение требований Федерального закона РФ от 26.07.2006 г. №152-ФЗ "О персональных данных", а также иных нормативных документов по защите информации **приказываю:**

1. Утвердить инструкцию о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (прилагается).
2. Руководителям структурных подразделений ознакомить с указанной Инструкцией сотрудников подразделений обрабатывающие персональные данные.
3. Ознакомить с настоящим приказом заинтересованных лиц (отв. Свиридова Д.С.).
4. Ответственность за исполнение данного приказа возложить на руководителей структурных подразделений.
5. Контроль исполнения приказа возложить на первого проректора проректор по основной деятельности Стефанову Г.П.

И.о. ректора А.П. Лунёв

Первый проректор, проректор по основной деятельности Г.П. Стефанова

Первый проректор, проректор по ЭФиР Т.М. Храмова

Начальник УД А.Ф. Бурукина

Начальник УМУ Т.В. Степкина

Начальник УТиВТ Б.Р. Досмухамедов

Начальник ЮО Д.Г. Чалов

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный университет» (Астраханский государственный университет)

УТВЕРЖДЕНА

Приказом и.о. ректора АГУ
от «28» 08 2015 г.
№ 0801-01/742

Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

1. Общие положения

1.1. Настоящей Инструкцией определяются обязательные для всех структурных подразделений университета требования по обеспечению конфиденциальности документов, содержащих персональные данные.

1.2. Для целей настоящей Инструкции используются следующие основные понятия:

- «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;
- «Оператором», организующим и осуществляющим обработку персональных данных, является федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный университет» (далее - Университет);
- «Конфиденциальная информация» – это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

1.3. Нормативные документы, определяющие основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных и использования средств автоматизации (Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации". Обработка

персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее);

1.4. Обеспечение конфиденциальности персональных данных не требуется в случае их обезличивания или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники), в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, занимаемая должность и место работы, ученая степень, ученое звание, сведения о квалификации, профессии - для сотрудников; курс, группа, факультет, специальность, данные об обучении – для студентов и иные персональные данные, предоставленные субъектом персональных данных.

1.5. Обработка персональных данных допускается с согласия субъекта персональных данных на обработку его персональных данных;

1.6. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных путем подачи письменного заявления.

1.7. Порядок ведения перечней персональных данных.

1.7.1. В структурных подразделениях Университета должны формироваться и вестись перечни персональных данных с указанием регламентирующих документов, мест хранения и ответственных за обработку и хранение данных (**Приложение №1**).

1.7.2. Осуществлять обработку и хранение персональных данных, не внесенных в перечень, запрещается.

1.8. Общие правила хранения и передачи персональных данных.

1.8.1. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

1.8.2. Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные, запрещается.

1.8.3. Передача персональных данных допускается только в случаях, установленных Федеральным законам Российской Федерации «О персональных данных», а также по письменному поручению (резолюции) вышестоящих должностных лиц.

1.8.4. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.9. Ответственность за защиту обрабатываемых персональных данных

1.9.1. Лица, осуществляющие обработку и хранение персональных данных, несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных

данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.
1.9.2. Сотрудники Университета, допущенные к обработке персональных данных, должны быть в обязательном порядке ознакомлены под роспись с настоящей Инструкцией.
1.9.3. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается на руководителей структурных подразделений Университета.

2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации

2.1. Условия хранения персональных данных.

2.1.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.
2.1.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.
2.1.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
2.1.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию.
2.2. Использование типовых форм документов и журналов учета.

2.2.1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:
а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Оператора;

б) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
в) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.
2.2.2. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:
а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Оператор.
2.3. Порядок уничтожения или обезличивания персональных данных.

2.3.1. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
2.3.2. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации.

3.1. Правила доступа, хранения и пересылки персональных данных.

3.1.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

3.1.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.
3.1.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.
3.1.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.
3.1.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.
3.2. Общие требования по защите персональных данных в автоматизированных системах.
3.2.1. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.
3.2.2. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:
а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.
3.2.3. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:
а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;
в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
д) описание системы защиты персональных данных.

3.2.4. Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту в «Журнале учета съемных носителей персональных данных» (Приложение №2).

4.2. При использовании съемных носителей персональных данных запрещается:

• хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

• выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

4.3. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенным адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.4. Съемные носители подлежат периодической проверке на вирусы и вредоносное программное обеспечение администратором, ответственным за защиту персональных данных.

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт.

4.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт (приложение № 3)

Начальник УД А.Ф. Бурукина

Начальник УТиВТ Б.Р. Досмухамедов

Начальник ЮО Д.Г. Чалов

Приложение № 1

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в структурных подразделениях федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Астраханский государственный университет»

_____

(наименование структурного подразделения)

№ п\п	Наименование (вид, типовая форма) документов с персональными данными	Наименование информационной системы/ без использования средств автоматизации	Место хранения (комната)	ФИО ответственных за обработку и хранение
1				
2				
3				

_____ _____ _____

(должность) (ФИО начальника структурного подразделения) (подпись)

Приложение №2

ЖУРНАЛ

учета съемных носителей персональных данных

_____

(наименование структурного подразделения)

Начат «__» _____ 20___ г.

Окончен «__» _____ 20___ г.

_____

Должность и ФИО ответственного за хранение

_____

Должность и ФИО администратора

№ п/п	Наименование и номер съемного носителя	Фамилия исполнителя	Действие (Получил, вернул, проверил)	Дата и время действия	Подпись исполнителя	Подпись ответственного за хранение
1						
2						
3						
4						
5						

Приложение № 3

«УТВЕРЖДАЮ»

_____ _____

« »_____ 200 г.

АКТ

уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом _____ от № в составе:

_____

(должности, ФИО)

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
	2	3	4

Всего съемных носителей_____

(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены

_____

путем (разрезания, демонтажа и т.п.) ,

_____

измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья

_____ _____

(наименование предприятия) (Дата)

Председатель комиссии Подпись Дата

Члены комиссии

(ФИО) Подпись Дата