Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный автомобильно-дорожный университет (СибАДИ)"

УТВЕРЖДЕНО
и введено в действие
приказом П-22-19/01 от 25.01.2022
И.о. ректора ФГБОУ ВО «СибАДИ»
А.П. Жигадло
«25» января 2022 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ИНСТРУКЦИЯ

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

СМК ЦТиВТ- И-1- 2022

Издание официальное

Экз. № 1 из 2

1. Общие положения

1.1. Настоящая Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее-Инструкция) Федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный автомобильно-дорожный университет (СибАДИ)» (далее - ФГБОУ ВО «СибАДИ», Университет) разработана соответствии с:

- Федеральным законом Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных» (далее по тексту: 152-ФЗ);
- Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
- Постановлением правительства РФ от 15.09.2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Положением об обработке персональных данных в ФГБОУ ВО «СибАДИ», утв. 29.10.2021г.;
- Политикой в отношении обработки персональных данных в ФГБОУ ВО «СибАДИ», утв. 23.01.2018г.

1.2. Настоящая Инструкция вступает в силу с момента ее утверждения ректором Университета.

1.3. Все изменения в Инструкцию вносятся приказом ректора Университета.

1.4. Все работники Университета участвующие в обработке персональных данных (далее - обработчики ПДн), должны быть ознакомлены с настоящей Инструкцией под подпись.

2. Цель

2.1. Целью разработки настоящей Инструкции является определение обязательных для всех работников, обрабатывающих персональные данные в Университете, требований по обеспечению конфиденциальности информации, содержащей персональные данные, в соответствии законодательством Российской Федерации при использовании и хранении персональных данных работников, обучающихся, выпускников, других категорий субъектов персональных данных.

3. Основные понятия

3.1. В настоящей Инструкции используются понятия:

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

2) персональные данные, разрешенные субъектом персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

3) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Под оператором персональных данных в данной Инструкции подразумевается ФГБОУ ВО «СибАДИ»;

4) 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;

5) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

6) конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным субъектов, требование не допускать распространения без согласия субъекта или иного законного основания.

Конфиденциальность относительно обработки персональных данных и защите частной жизни в электронном коммуникационном секторе заключается в запрете просмотра, записи или хранения, а также других способах вмешательства или наблюдения за сообщениями и относящимся к ним данным по трафику, осуществляемые лицами или другими пользователями без согласия самого пользователя;

7) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

8) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

9) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

10) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых
уничтожаются материальные носители персональных данных;

11) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

12) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

13) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Примечание. Понятие общедоступных персональных данных исключено Федеральным законом от 30.12.2020 N 519-ФЗ "О внесении изменений в Федеральный закон "О персональных данных".

4. **Обозначения и сокращения**

4.1. В настоящей Инструкции применяются следующие обозначения сокращения:

ПДн - персональные данные;

ФГБОУ ВО «СибАДИ» - Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный автомобильно-дорожный университет (СибАДИ)»;

СМК - система менеджмента качества;

ПЭВМ - персональная электронно-вычислигельная машина:

ответственное лицо (ответственный работник) - лицо, ответственное за обработку ПДн в подведомственных ему помещениях;

посторонние лица - работники, в чьи служебные обязанности не входит обработка используемых ПДн, и лица, не являющиеся субъектами обрабатываемых ПДн.

5. Доступ работников Университета или третьих лиц к ПДн

5.1. К обработке ПДн, в пределах своих должностных обязанностей, допускаются работники Университета, на которых оформлен соответствующий допуск.

5.2. Работник Университета получает допуск к обработке ПДн после изучения Политики, Положения, локальных нормативных актов Университета, касающихся обработки персональных данных, и принятия Обязательства о неразглашении персональных данных, ставших ему известными при выполнении его служебных обязанностей.

5.3. Работники Университета, допущенные к обработке ПДн, имеют право доступа только к тем ПДн, которые необходимы им для выполнения конкретных трудовых функций.

5.4. В случае если на основании заключенных договоров (либо иных оснований) Университета с третьими лицами, третьи лица могут получить доступ к ПДн, то существенным условием заключенного договора является обязанность обеспечения третьими лицами конфиденциальности, ставших им известными при выполнении договора.

5.5. На обезличенные ПДн не распространяются требования по обеспечению конфиденциальности.

6. Распространение персональных данных

6.1. В соответствии со ст. 7 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.2. Чтобы передать персональные данные конкретному лицу или лицам, необходимо получить согласие на обработку персональных данных и указать в качестве действия с персональными данными их предоставление.

Другой вариант – получить согласие на распространение персональных данных и указать в нем передачу конкретным лицам в качестве ограничения (п.6 ч.1 ст.3, ст.9 152-ФЗ).

6.3. При необходимости передачи персональных данных работника неограниченному кругу лиц, необходимо получить у него письменное Согласие на распространение персональных данных. Согласие на обработку в этом случае не подойдет (ст.88 ТК, ст.10.1 152-ФЗ, приказ РКН от 24.02.2021 №18).

6.4. Если физическое лицо подписало согласие на обработку персональных данных, но не дало своего согласия на их распространение, оператор может их обрабатывать (хранить, уточнять, использовать и т.д.), но не имеет права передавать их кому-либо еще (п.4 ст.10.1 152-ФЗ). Это не касается передачи персональных данных государственным структурам, то есть военкомату, ФНС, ФСС, полиции, следственным органам и т.д. Персональные данные физического лица можно передавать им без его согласия (пп.2 – 11 ч.1 ст.6 152-ФЗ).

6.5. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на распространение его персональных данных (п.8 ст. 10.1 152-ФЗ).

6.6. Согласие на распространение может быть предоставлено оператору персональных данных (п.6 ст.10.1 152-ФЗ):

- непосредственно на бумаге с личной подписью;
- через информационную систему Роскомнадзора.

6.7. Уведомлять Роскомнадзор о намерении начать обработку персональных данных, разрешенных для распространения, не нужно (пп.4 и п.2 ст.22 152-ФЗ).

6.8. Согласие на распространение персональных данных приведено в Приложении 7 к Положению об обработке персональных данных.

6.9. Субъект персональных данных наделен правом самостоятельно выбирать, какие именно персональные данные и на каких условиях может распространять оператор, получивший к ним доступ (в п.9 ст. 10.1 152-ФЗ).

Например, он может разрешить опубликовать только его фото и Ф.И.О., а дату рождения запретить публиковать.

Либо он может разрешить передачу персональных данных третьим лицам, но только при условии, что они являются работниками Университета.

6.10. Установленные субъектом персональных данных запреты и условия их обработки не действуют, когда их обработка осуществляется в государственных, общественных или иных публичных интересах (п.11 ст.10.1 152-ФЗ). Например, несмотря на запрет, оператор может передать персональные данные в налоговую, ПФР, военкомат, полицию, следственный комитет и т.д.

6.11. Если в согласии прямо не указано, что субъект персональных данных не установил запреты и условия обработки персональных данных, их не следует передавать неограниченному кругу лиц (ч.5 ст.10.1 152-ФЗ).

6.12. Нельзя распространять общедоступные персональные данные без согласия субъекта персональных данных. Даже если субъект самостоятельно разместил в общедоступном месте (например, в социальных сетях) свои персональные данные, взять их оттуда для дальнейшей обработки и распространения прямо запрещено законом. Каждое лицо, обрабатывающее или распространяющее размещенные самим субъектом персональные данные, должно доказать законность их обработки, поэтому даже в этом случае понадобится письменное согласие субъекта персональных данных на обработку и/или распространение его персональных данных (п.2 ст.10.1 152-ФЗ).

6.13. Третьи лица должны быть оповещены о запретах и условиях обработки персональных данных

6.14. Получив согласие на распространение персональных данных, содержащее условия или запреты на их обработку, оператор должен опубликовать информацию о таких условиях или запретах в течение трех рабочих дней (п.10 ст.10.1 152-ФЗ). Информация должна быть опубликована и доступна в том же месте, где опубликованы персональные данные (например, на той же веб-странице, на которой размещены фото и Ф.И.О. гражданина).

7. Отзыв согласия на распространение персональных данных

7.1. Субъект может отозвать согласие на распространение персональных данных

Оператор персональных данных обязан прекратить распространение (передачу, предоставление, доступ) персональных данных по требованию субъекта персональных данных. Для этого гражданин должен написать заявление об отзыве согласия на их распространение (п.12 ст. 10.1 152-ФЗ; Приложение 8 к Положению об обработке персональных данных).

7.2. Прекратить распространение нужно в течение трех рабочих дней с момента получения заявления. В противном случае субъект персональных данных вправе обратиться в суд с этим же требованием (п.14 ст.10.1 152-ФЗ).

7.3. Все перечисленные выше правила обработки персональных данных полностью распространяются на процесс обработки персональных данных работников работодателями. Это означает, что для распространения персональных данных работников (например, для размещения их на сайте работодателя) при приеме на работу или после заключения трудового

договора необходимо брать с работника дополнительное согласие на распространение его персональных данных. В противном случае персональные данные работника можно будет передать только при наличии условий, когда согласие работника на их передачу не требуется.

7.4. Передавать персональные данные работника в банк с целью оформления зарплатной карты без согласия работника можно только в исключительных случаях, а именно:

- когда договор заключается непосредственно между банком и работником;
- когда у работодателя есть доверенность на представление интересов работника в банке;
- когда выплата зарплат на банковскую карту работника предусмотрена коллективным договором.

8. **Меры, обеспечивающие сохранность носителей ПДн в нерабочее время**

8.1. Мерами, предпринятыми в Университете, для обеспечения сохранности носителей ПДн, в нерабочее время, являются:

- круглосуточная охрана;
- сигнализация;
- решетки в оконных проемах;
- двери, являющиеся надежным препятствием для проникновения в помещения.

8.2. Дополнительно, для Управления правового и кадрового обеспечения предусмотрено опечатывание помещений.

8.3. Общие меры по соблюдению конфиденциальности ПДн:

8.3.1. Лица, не включенные в список лиц, имеющих право доступа в кабинет, не должны оставаться одни в помещении.

8.3.2. О факте утраты носителей информации, удостоверений, пропуске ключей от защищенных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению персональных данных, необходимо немедленно сообщить руководителю структурного подразделения и главному специалисту по комплексной защите информации.

8.3.3. Уборка помещения, где обрабатываются ПДн, должна проводиться под контролем лица, ответственного за обработку персональных данных в данном подразделении.

8.3.4. По окончании рабочего дня, работник, ответственный за обработку ПДн, должен закрыть все форточки, активировать сигнализацию,

запереть помещение на ключ и, если предусмотрено опечатывание, опечатать кабинет.

9. Правила работы с бумажными носителями ПДн

9.1. Общие правила по работе с бумажными носителями ПДн:

9.1.1. ПДн могут содержаться только в типовых формах, содержащихся «Перечне типовых форм документов, использующихся в структурном подразделении Университета, предполагающих или допускающих содержание ПДн» и в объеме, предусмотренном этими типовыми формами.

9.1.2. Не допускается бесконтрольно оставлять бумажные носители ПДн.

9.1.3. Бумажные носители ПДн, по завершению работы с ними, должны быть помещены на прежнее место.

9.2. Правила хранения бумажных носителей ПДн

9.2.1. Хранение бумажных носителей ПДн допускается исключительно в контейнерах бумажных носителей (папки, подшивки), способами, позволяющими в кратчайший срок определить места хранения требующихся персональных данных.

9.2.2. Бумажные носители ПДн, содержащие различные категории и/или цели обработки ПДн, необходимо хранить в различных контейнерах бумажных носителей (папки, подшивки).

9.3. Правила внесения уточнений в ПДн, содержащихся на бумажных носителях ПДн.

9.3.1. Внесение уточнений в ПДн, содержащихся на бумажных носителях ПДн, производится посредством вычеркивания или замазывания пастой-штрих этих ПДн с последующей подписью субъекта этих ПДн.

9.3.2. Если внесение уточнений не позволяют технические особенности бумажного носителя ПДн, то этот носитель передается субъекту ПДн, а вместо него изготавливается новый бумажный носитель с уточненными ПДн.

9.4. Порядок уничтожения бумажных носителей ПДн

9.4.1 Бумажные носители ПДн подлежат уничтожению по достижению целей обработки, по истечению срока обработки или в случае утраты необходимости в их достижении, если иное не предусмотрено федеральными законами.

9.4.2. Уничтожение бумажных носителей ПДн необходимо производи' способами, исключающими возможность последующего использования содержащихся на них ПДн.

9.4.3. По факту уничтожения бумажных носителей ПДн составляется акт об уничтожении бумажных носителей ПДн.

Комиссия по уничтожению состоит из трех человек, двух назначает руководитель подразделения, а одного - вышестоящий руководитель.

Акт об уничтожении бумажных носителей ПДн хранится постоянно в подразделении, в котором хранились уничтоженные бумажные носители ПДн.

10. Порядок передачи ПДн третьим лицам

10.1. Передача ПДн по каналам связи, не контролируемым СибАДИ, допускается в следующие организации:

- пенсионный фонд;
- банки;
- управление федерального казначейства;
- инспекцию федеральной налоговой службы

Передача ПДн разрешается только с применением клиентских частей программных средств, используемых в этих организациях.

10.2. Передача ПДн по телефону, факсу или электронной почте без письменного согласия субъекта этих ПДн, запрещается.

11. Защита ПДн от утечки по видовым каналам

11.1. В целях предотвращения просмотра информации с монитора лицами, находящимися за пределами Университета, оконные проемы необходимо оборудовать устройствами типа жалюзи или плотными шторами.

11.2. Мониторы необходимо размещать таким образом, чтобы был исключен несанкционированный просмотр с них конфиденциальной информации, в том числе ПДн, посторонними лицами, находящимися в помещении.

11.3. Помещения, в которых допустимо постоянное нахождение посторонних лиц, необходимо оборудовать огораживающими стойками, отделяющими посторонних лиц от работников, занимающихся обработкой ПДн.

11.4. При возникновении угрозы просмотра ПДн посторонними лицами, необходимо прекратить обработку ПДн, свернуть окна приложений, содержащих ПДн, а бумажные носители ПДн перевернуть лицевой (информативной) стороной вниз.

12. Правила эксплуатации съемных носителей информации

12.1. Выдачу съемных носителей информации и принятие их обратно на хранение, с внесением соответствующих записей в журнале учета съемных носителей ПДн, должен осуществлять руководитель подразделения.

12.2. Съемные носители информации, использующиеся для временного или постоянного хранения ПДн, должны быть маркированы.

12.3. Вынос съемных носителей ПДн. для непосредственной передачи третьим липам, осуществляется после внесения соответствующей записи в журнале учета съемных носителей ПДн с занесением в колонку «Примечания» информации о Третьем лице, которому был передан носитель ПДн.

12.4. Не допускается бесконтрольно оставлять съемные носители информации.

12.5. О факте утраты съемных ностелей информации необходимо немедленно сообщить руководителю подразделения и главному специалисту по комплексной защите информации.

12.6. На утраченные носители информации составляется акт. Соответствующие отметки вносятся в журнал учета съемных носителей персональных данных.

12.7. По результатам уничтожения, пришедших в негодность, съемных носителей информации, составляется акт уничтожения съемных носителей ПДн.

12.8. Уничтожение съемных носителей информации необходимо производить механическими способами, исключающими возможность последующего восстановления информации с этих носителей.

12.9. Уничтожение съемных носителей информации производит комиссия по уничтожению, состоящая состоит из трёх человек: двух назначает руководитель подразделения, а одного - вышестоящий руководитель.

12.10. Комиссия составляет акт об уничтожении съемных носителей ПДн, который хранится постоянно в подразделении, в котором хранились уничтоженные съемные носители информации.

13. Порядок инициирования работ по ремонту или модернизации ПЭВМ

13.1. При необходимости проведения работы по ремонту или модернизации ПЭВМ, предназначенных для хранения или обработки ПДн,

составляется служебная записка на имя начальника ЦТиВТ, в которой указывается:

- инвентарный номер ПЭВМ, модернизацию или ремонт которой необходимо провести;
- номер кабинета, в котором ПЭВМ функционирует;
- ФИО постоянного пользователя (обработчика ПДн);
- перечень ПДн, которые обрабатываются на данной ПЭВМ;
- если необходима модернизация, то с какой целью.

13.2. Служебная записка согласовывается с начальником отдела или его заместителем.

14. Обязанности должностных лиц

14.1. Требования, предъявляемые настоящей Инструкцией и «Положением об обработке ПДн», обязаны выполнять работники Университета, как выполняющие все виды обработки ПДн, так и имеющие к ним доступ для принятия решений.

15. Ответственность

15.1. Обработчики ПДн несут персональную ответственность за все действия, производимые ими с ПДн в соответствии с Законодательством РФ, в том числе:

- незаконное разглашение или использование персональных данных без согласия субъекта этих персональных данных, из корыстной или иной личной заинтересованности ст. 183, 137 УК РФ, ст. 13.14, 13.1 1 КоАП РФ;
- преднамеренное или не преднамеренное нарушение настоящей Инструкции или Положения об обработке ПДн ст. 274. 293 УК РФ, ст. 90 ТК РФ.

15.2. Обработчики ПДн несут полную материальную ответственность в случаях незаконного разглашения или использования персональных данных, полученных ими при выполнении служебных обязанностей, а также в случае причинения своими действиями ущерба Университету» (ст. 243 ТК РФ).

15.3. Обработчикам ПДн запрещается передавать:

- свои логины и пароли на вход в операционную систему при включении компьютера или ноутбука, а также при выходе компьютера или ноутбука из «сна» и блокировки;
- пароли от рабочих баз с персональными данными.

Обработчики ПДн несут персональную административную ответственность за разглашение этой служебной информации.

Разработчик:
главный специалист
по комплексной защите информации Л.Е.Олейник

ЛИСТ СОГЛАСОВАНИЯ

Согласовано:

Проректор по ИТ
«18» января 2022г. _____ В.А.Мещеряков

Начальник УПиКО
«18» января 2022г. _____ Т.В.Каменская

Начальник ЦТиВТ
«18» января 2022г. _____ В.О.Чариков

Уполномоченный по СМК
«17» января 2022г. _____ И.А. Стуцаренко

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ

№ изменения	Дата распорядительного документа о внесении изменений, содержание изменения	Ф.И.О. и подпись лица, внёсшего изменения	Дата

ЛИСТ ОЗНАКОМЛЕНИЯ И СОГЛАСИЯ

№	Ф.И.О.	Должность	Подпись