МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»
(ГУАП)

ГУАП
№ 05-78/25
от 17.02.2025

ПРИКАЗ

17.02.2025 № 05-78/25

Об утверждении инструкции пользователя информационных систем персональных данных ГУАП

В целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию пользователя информационных систем персональных данных ГУАП (Приложение к настоящему приказу).
2. Руководителям структурных подразделений, осуществляющим обработку персональных данных, ознакомиться самим и обеспечить (обеспечивать) ознакомление с Инструкцией подчиненных работников, в чьи должностные обязанности входит обработка персональных данных, в течение 10 рабочих дней с даты издания настоящего приказа. Листы ознакомления направить начальнику Управления цифрового развития Трифоновой Ю.В.
3. Контроль за исполнением настоящего приказа возложить на проректора по административной работе и безопасности Павлова И.А.

Ректор Ю.А. Антохина

Приложение к приказу ГУАП
от «17» 02 2025 г. № 05-78/25

Инструкция пользователя
информационных систем персональных данных ГУАП

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Пользователем информационных систем персональных данных (далее – Пользователь) является уполномоченный работник ГУАП.

1.2. Пользователь должен знать нормы законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных (далее – ПДн).

1.3. В своей деятельности, связанной с обработкой ПДн, Пользователь руководствуется Политикой обработки персональных данных в ГУАП и настоящей Инструкцией.

1.4. Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой информации, несут персональную ответственность за свои действия.

2. ОБЯЗАННОСТИ И ПРАВА ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Пользователь обязан:

– соблюдать требования Политики обработки персональных данных в ГУАП и иных локальных нормативных актов ГУАП, устанавливающих порядок работы с ПДн;

– выполнять в информационных системах персональных данных (далее – ИСПДн) только те процедуры, которые необходимы для исполнения его должностных обязанностей;

– использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера;

– пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;

– обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;

– немедленно сообщать руководителю структурного подразделения или ответственному за обеспечение информационной безопасности ПДн в ИСПДн (далее – Ответственный) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

– перед началом обработки в ИСПДн файлов, хранящихся на съемных машинных носителях информации, осуществлять проверку файлов на наличие компьютерных вирусов;

– располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

– соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.

2.2. Пользователям ИСПДн запрещается:

– записывать и хранить информацию, относящуюся к конфиденциальной информации или ПДн, на неучтенных материальных носителях информации;

– оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка информации;

– отключать средства антивирусной защиты;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

– самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

– обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИСПДн;

– сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИСПДн;

– работать в ИСПДн при обнаружении каких-либо неисправностей;

– хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

– вводить в ИСПДн ПДн под диктовку или с микрофона;

– привлекать посторонних лиц для производства ремонта технических средств ИСПДн без согласования с Ответственным.

2.3. Пользователь имеет право знакомиться с внутренними документами ГУАП, регламентирующими его обязанности по занимаемой должности.

3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ПО ПАРОЛЬНОЙ ЗАЩИТЕ

3.1. Пользователям запрещается:

– записывать свои пароли в очевидных местах, таких как внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

– хранить пароли в записанном виде на отдельных листах бумаги;

– сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от несанкционированного доступа.

3.2. Плановую смену паролей Пользователь осуществляет при истечении максимального срок действия пароля или заблаговременно до наступления окончания срока действия пароля.

3.3. При обнаружении фактов утраты, компрометации (подозрении на компрометацию) ключевой, парольной и аутентифицирующей информации Пользователь обязан незамедлительно сообщить об этом Ответственному.

3.4. Внеплановая смена личного пароля Пользователем должна производиться в следующих случаях:

– компрометация (подозрение на компрометацию) пароля;

– по инициативе Пользователя;

– по инициативе Ответственного.

4. ТЕХНОЛОГИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. При первичном допуске к работе с ИСПДн Пользователь:

– проходит инструктаж по использованию ИСПДн;

– знакомится с требованиями законодательства Российской Федерации в области обработки и обеспечения безопасности ПДн;

– получает у работника, выполняющего функции по управлению (администрированию) системой защиты персональных данных, идентификатор и начальную аутентификационную информацию (пароль) для входа в ИСПДн.

4.2. Перед началом работы Пользователь визуально проверяет целостность пломб, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.

4.3. Авторизацию в ИСПДн (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.

4.4. В процессе работы на АРМ ИСПДн Пользователь использует технические средства и установленное Ответственным программное обеспечение согласно техническому паспорту ИСПДн.

4.5. Копирование ПДн на машинные носители информации осуществляется только при наличии производственной необходимости и только на учтенные машинные носители информации.

4.6. При необходимости создания на АРМ Пользователя дополнительных электронных документов, содержащих ПДн, Пользователь создает и хранит такие документы в строго отведенном для этого месте.

4.7. Печать документов, содержащих ПДн, осуществляется только при наличии производственной необходимости. Все бумажные носители, не подлежащие учету по каким-либо техническим или иным причинам (сбой принтера при печати, обнаружение ошибок в документе после распечатки и т.д.) уничтожаются незамедлительно. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих ПДн, уничтожаются незамедлительно после подписания (утверждения) окончательного варианта документа.

4.8. В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИСПДн, Пользователь обязан выключить компьютер либо заблокировать его. Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других работников ГУАП, Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.

4.9. Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.

ЛИСТ ОЗНАКОМЛЕНИЯ

с Инструкцией пользователя информационных систем персональных данных ГУАП

№ п/п	ФИО	Должность	Дата	Подпись