

Министерство
сельского хозяйства РФ

ФГБОУ ВО
Кабардино-Балкарский
государственный
аграрный
университет
имени В.М. Кокова

Приказ

03.12.2025г. № 328/О
г. Нальчик

Об утверждении Порядка доступа сотрудников в помещения, в которых ведется обработка защищаемой информации, в т. ч. персональных данных, на объекте информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России»

Во исполнение приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации № 1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», **П Р И К А З Ы В А Ю:**

1. Утвердить Порядок доступа сотрудников в помещения, в которых ведется обработка защищаемой информации, в том числе персональных данных, на объекте информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России» (далее – ИСПДн для подключения к ЗСПД) в соответствии с Приложением.

2. Контроль за исполнением настоящего приказа оставляю за собой.

Основание: представление инженера-программиста Хотова А.Л., визы: проректора по НР Беровой Д.М., проректора по УР и ЦТ Красовской О.А., проректора по РИ Бозиева Ю.М., начальника ФЭУ Кадыкоева М.А., начальника ЮО Малуховой Р.Х.

Ректор

З.Л. Шхагапсоев

Визы:

Проректор по НР

Д.М. Берова

Проректор по УР и ЦТ

О.А.Красовская

Проректор по РИ

Ю.М. Бозиев

Начальник ФЭУ

М.А. Кадыкоев

Начальник ЮО

Р.Х. Малухова

Порядок доступа сотрудников в помещения, в которых ведется обработка защищаемой информации, в т. ч. персональных данных, на объекте информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России»

1 Общие положения

1.1 Настоящий Порядок доступа сотрудников в помещения, в которых ведется обработка защищаемой информации, в т. ч. персональных данных, на объекте информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России» (далее – ИСПДн для подключения к ЗСПД) определяет правила доступа сотрудников в помещения, в которых ведется обработка защищаемой информации, в т. ч. персональных данных, в рабочее и нерабочее время, а также в нештатных ситуациях; перечень помещений, предназначенных для обработки защищаемой информации, в т. ч. персональных данных, ИСПДн для подключения к ЗСПД и перечень лиц, имеющих право доступа в помещения с элементами ИСПДн для подключения к ЗСПД.

1.2 Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками, допущенными к обработке информации в ИСПДн для подключения к ЗСПД.

1.3 Ответственность за соблюдение требований настоящего Порядка несут сотрудники структурных подразделений Учреждения, участвующих в обработке защищаемой информации, в т. ч. персональных данных, в ИСПДн для подключения к ЗСПД, а также руководители данных структурных подразделений.

1.4 Контроль соблюдения требований настоящего Порядка обеспечивает ответственный за защиту информации в ИСПДн для подключения к ЗСПД.

2 Требования к помещениям, в которых ведется обработка защищаемой информации, в т. ч. персональных данных, ИСПДн для подключения к ЗСПД

2.1 Бесконтрольный доступ посторонних лиц в помещения с элементами ИСПДн для подключения к ЗСПД должен быть исключён.

2.2 Все помещения ИСПДн для подключения к ЗСПД должны быть оборудованы входными дверьми с замками, запирающимися на ключ, и приспособлениями для опечатывания, либо соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений. Особое внимание при оснащении техническими средствами, препятствующими осуществлению несанкционированного проникновения или пребывания, рекомендуется уделить помещениям, в которых будут расположены СКЗИ.

3 Организация порядка по режиму допуска в помещения, в которых обработка защищаемой информации, в т. ч. персональных данных, ИСПДн для подключения к ЗСПД

3.1 Должен быть определен перечень помещений, предназначенных для обработки защищаемой информации, в т. ч. персональных данных, ИСПДн для подключения к ЗСПД (Приложение 1), и организован контроль доступа сотрудников и посетителей в помещения,

в которых установлены технические средства (далее - ТС) ИСПДн для подключения к ЗСПД

и осуществляется обработка защищаемой информации, в т. ч. персональных данных, а также хранятся машинные носители информации.

Необходимо разработать схему границ контролируемой зоны ИСПДн для подключения

к ЗСПД, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию и средства защиты информации, а также средства обеспечения функционирования.

3.2 Доступ сотрудников структурных подразделений Учреждения в помещения, в которых осуществляется обработка защищаемой информации, в т. ч. персональных данных, организовывается на основании перечня лиц, имеющих право доступа в помещения с элементами ИСПДн для подключения к ЗСПД (Приложение 2).

3.3 Доступ посторонних лиц в помещения ИСПДн для подключения к ЗСПД, должен осуществляться только ввиду служебной необходимости. Данные лица допускаются в помещения только по согласованию с начальником структурного подразделения и с разрешения администратора безопасности ИСПДн для подключения к ЗСПД и имеют право пребывания в помещениях только под контролем ответственных лиц

3.4 На момент присутствия посторонних лиц в помещениях ИСПДн для подключения

к ЗСПД, должны быть приняты меры по недопущению ознакомления посторонних лиц с защищаемой информацией (например: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).

3.5 В нерабочее время помещения ИСПДн для подключения к ЗСПД должны запираются

на ключ и опечатываться или ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, съемные носители информации должны быть убраны в запираемые шкафы (сейфы), АРМ и принтер выключены. В случае оснащения помещения техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений, помещение сдается под охрану.

3.6 Устройства вывода (отображения) информации (экраны мониторов автоматизированных рабочих мест пользователей, а также принтеры) должны быть расположены так, что возможность несанкционированного просмотра выводимой на них информации исключается.

Двери в помещения имеют надежные замки, закрывающиеся на ключ.

Окна помещений должны быть оснащены непрозрачными жалюзи (шторами).

Пользователи должны быть проинструктированы о работе в ИСПДн для подключения

к ЗСПД, в т.ч. и о расположении мониторов АРМ.

Реализованный в ИСПДн для подключения к ЗСПД механизм защиты технических средств должен соответствовать требованиям, предъявляемым к информационным системам, для которых установлена необходимость обеспечения четвертого уровня защищенности персональных данных.

3.7 Для защиты помещений, в которых расположены ТС ИСПДн для подключения к ЗСПД, должны приниматься меры для минимизации воздействий огня (оборудованы датчиками охранно-пожарной сигнализации), воды, пыли, а также кражи.

3.8 ТС ИСПДн для подключения к ЗСПД и размещенное совместно с ними вспомогательное оборудование должны подвергаться регулярным осмотрам с целью выявления изменения конфигурации средств электронно-вычислительной техники (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.).

3.9 Работники и должностные лица Учреждения, получившие доступ к ИСПДн для подключения к ЗСПД не должны покидать помещение, в котором ведется обработка защищаемой информации, в т. ч. персональных данных, оставляя в нем без присмотра посторонних лиц, включая сотрудников Учреждения, не уполномоченных на обработку защищаемой информации, в т. ч. персональных данных.

3.10 Дистрибутивы с ОС и прикладным ПО, а также дистрибутивы СЗИ и их дубликаты должны храниться у администратора безопасности.

Приложение №1

**к Порядку доступа сотрудников в помещения, в которых ведется
обработка защищаемой информации, в т. ч. персональных данных
ИСПДн для подключения к ЗСПД**

**Перечень помещений, предназначенных для обработки защищаемой информации,
в т. ч. персональных данных на объекте информатизации – «Информационная
система персональных данных Федерального государственного бюджетного
образовательного учреждения высшего образования «Кабардино-Балкарский
государственный аграрный университет имени В.М. Кокова» для подключения
к защищенной сети передачи данных информационным системам и ресурсам ИТКИ
Минобрнауки России»**

№ п/п	№ кабинета, помещения	Адрес расположения
1.	Кабинет № 402	360030, Кабардино-Балкарская Республика, г. Нальчик, пр. Ленина, 1в., корпус 10, этаж 4

Приложение 2
к Порядку доступа сотрудников в помещения, в
которых ведется обработка защищаемой информации,
в т. ч. персональных данных ИСПДн для подключения
к ЗСПД

Перечень лиц, имеющих право доступа в помещения с элементами объекта информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России»

№ п/п	Фамилия, имя, отчество	Должность	Наименование отдела, № помещения	Ознакомлен (Дата, подпись)
1.	Бозиев Юсуф Мухарбиевич	Проректор по развитию инфраструктуры	Центр международного сотрудничества, Кабинет № 402	
2.	Хотов Азамат Лионович	Инженер-программист	Центр международного сотрудничества, Кабинет № 402	
3.	Шуляк Александр Борисович	Ведущий инженер	Центр международного сотрудничества, Кабинет № 402	
4.	Шуляк Александр Борисович	Ведущий инженер	Центр международного сотрудничества, Кабинет № 402	
5.	Хотов Азамат Лионович	Ведущий инженер	Центр международного сотрудничества, Кабинет № 402	
6.	Лакунова Мадина Сафарбиевна	Начальник центра международного сотрудничества	Центр международного сотрудничества, Кабинет № 402	
7.	Лакунова Мадина Сафарбиевна	Начальник центра международного сотрудничества	Центр международного сотрудничества, Кабинет № 402	
8.				

Лист ознакомления

[illegible]

