Министерство
сельского хозяйства РФ

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

Приказ

03.12.2025г. № 325/О
г. Нальчик

Об утверждении инструкций 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»

П Р И К А З Ы В А Ю:

1. Утвердить Инструкцию ответственному за защиту информации и обеспечение защиты персональных данных при их обработке 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) (Приложение 1).
2. Ответственному за защиту информации и обеспечение защиты персональных данных при их обработке в ИСПДн для подключения к ЗСПД ознакомиться под роспись и руководствоваться в своей деятельности Инструкцией ответственному за защиту информации и обеспечение защиты персональных данных при их обработке в ИСПДн для подключения к ЗСПД.
3. Утвердить Инструкцию Администратору безопасности ИСПДн для подключения к ЗСПД (Приложение 2).
4. Утвердить Инструкцию администратору ИСПДн для подключения к ЗСПД (Приложение 3).
5. Утвердить Инструкцию о порядке работы пользователя в ИСПДн для подключения к ЗСПД (Приложение 4).
6. Утвердить Инструкцию по организации парольной защиты в ИСПДн для подключения к ЗСПД (Приложение 5).
7. Утвердить Инструкцию о действиях лиц, допущенных к работе в ИСПДн для подключения к ЗСПД, в случае возникновения нештатных ситуаций (Приложение 6).
8. Утвердить Инструкцию по организации резервного копирования в ИСПДн для подключения к ЗСПД (Приложение 7).
9. Утвердить Инструкцию по защите информации о событиях безопасности в ИСПДн для подключения к ЗСПД (Приложение 8).

10. Утвердить Инструкцию о порядке изменения состава и конфигурации технических и программных средств в ИСПДн для подключения к ЗСПД (Приложение 9).

11. Утвердить Инструкцию по обеспечению защиты информации при выводе из эксплуатации или после принятия решения об окончании обработки информации в ИСПДн для подключения к ЗСПД (Приложение 10).

12. Утвердить Инструкцию об использовании мобильных технических средств в ИСПДн для подключения к ЗСПД (Приложение 11).

13. Утвердить Инструкцию по организации антивирусной защиты в ИСПДн для подключения к ЗСПД (Приложение 12).

14. Ответственному за защиту информации и обеспечение защиты персональных данных при их обработке в ИСПДн для подключения к ЗСПД ознакомить под роспись администраторов
и пользователей ИСПДн для подключения к ЗСПД с инструкциями, представленными в приложениях к приказу.

15. Приказ довести до сотрудников Учреждения в части, касающейся.

16. 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

Приложение 1
к приказу № 325 от 03.12.2025г.

Инструкция ответственному за защиту информации и обеспечение защиты персональных данных при их обработке 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 Настоящая Инструкция определяет обязанности ответственного за защиту информации (далее – Ответственный за ЗИ) 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).

1.2 Ответственный за ЗИ назначается приказом руководителя Учреждения.

1.3 Ответственный за ЗИ в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России в области защиты информации, внутренними организационно-распорядительными документами.

1.4 Ответственный за ЗИ по всем вопросам, связанным с защитой информационных ресурсов ИСПДн для подключения к ЗСПД, действует в соответствии с положениями данной Инструкции и во взаимодействии с Администраторами ИСПДн для подключения к ЗСПД.

1.5 Ответственный за ЗИ по вопросам защиты информации курирует работу Администраторов ИСПДн для подключения к ЗСПД.

2 Должностные обязанности Ответственного за ЗИ

Ответственный за ЗИ в ИСПДн для подключения к ЗСПД:

2.1 Осуществляет планирование работ по защите информации в ИСПДн для подключения к ЗСПД.

2.2 Организует и проводит работы по подготовке организационных и распорядительных документов по защите информации.

2.3 Организует и проводит работы по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации.

2.4 Организует и проводит в установленном порядке расследование причин и условий появления нарушений защиты информации в ИСПДн для подключения к ЗСПД.

2.5 Осуществляет доведение до сведения пользователей и администраторов ИСПДн для подключения к ЗСПД требований действующих нормативно-правовых и законодательных актов Российской Федерации в области защиты информации.

2.6 Организует и руководит выполнением работ по комплексной защите информации в ИСПДн для подключения к ЗСПД, обеспечивая эффективное применение всех имеющихся организационных и инженерно-технических мер в целях защиты информации ограниченного доступа.

2.7 Обеспечивает контроль за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также

действующего законодательства при решении вопросов, касающихся защиты информации.

3 Права Ответственного за ЗИ

Ответственный за ЗИ в ИСПДн для подключения к ЗСПД имеет право:

3.1 Требовать от пользователей и администраторов ИСПДн для подключения к ЗСПД безусловного соблюдения установленной технологии обработки информации и выполнения требований локальных документов, регламентирующих вопросы обеспечения защиты информации.

3.2 Давать пользователям и администраторам ИСПДн для подключения к ЗСПД обязательные для исполнения указания и рекомендации по вопросам информационной безопасности (далее – ИБ).

3.3 Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации
и технических средств ИСПДн для подключения к ЗСПД.

3.4 Осуществлять взаимодействие с руководством Учреждения и персоналом ИСПДн для подключения к ЗСПД по вопросам обеспечения безопасности информации.

3.5 Запрашивать и получать от начальников и специалистов структурных подразделений Учреждения информацию и материалы, необходимые для организации своей работы.

3.6 Вносить на рассмотрение руководства предложения по улучшению состояния защиты информации в ИСПДн для подключения к ЗСПД.

3.7 Принимать участие в проведении мероприятий по контролю за обеспечением безопасности информации в ИСПДн для подключения к ЗСПД.

4 Ответственность

4.1 Ответственные за ЗИ, виновные в несоблюдении настоящей Инструкции, расцениваются как нарушители законодательства РФ в области защиты информации и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Ответственный за ЗИ Шуляк Александр Борисович

Приложение 2
к приказу № 325 от 03.12.2025г.

Инструкция Администратору безопасности
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

1 Общее положения

1.1 Настоящая Инструкция определяет обязанности Администратора безопасности 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 (далее – ИСПДн для подключения к ЗСПД).

1.2 Администратор безопасности назначается приказом № __ от «__» _____ 20__ г.

1.3 Администратор безопасности в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России, регламентирующими документами Учреждения и другими документами.

1.4 Администратор безопасности по вопросам обеспечения безопасности информации подчиняется ответственному за защиту информации.

1.5 Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое).

1.6 Администратор безопасности осуществляет методическое руководство пользователей ИСПДн для подключения к ЗСПД в вопросах обеспечения правильной работы с используемыми в ИСПДн для подключения к ЗСПД средствами защиты информации (далее - СЗИ).

1.7 Требования Администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн для подключения к ЗСПД.

1.8 Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн для подключения к ЗСПД, состояние и поддержание установленного уровня защиты ИСПДн для подключения к ЗСПД.

2. Задачи Администратора безопасности

2.1 Основными задачами Администратора безопасности являются:

– поддержание необходимого уровня защиты ИСПДн для подключения к ЗСПД от несанкционированного доступа (НСД) к информации, в т.ч. ПДн;

– обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации, в т. ч. ПДн;

– установка средств защиты информации на элементах ИСПДн для подключения к ЗСПД
и контроль выполнения правил их эксплуатации;

– сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) ИСПДн для подключения к ЗСПД;

– периодическое обновление СЗИ (при необходимости);

– проведение комплекса мероприятий по предотвращению инцидентов ИБ;

– оперативное реагирование на нарушения требований по ИБ в ИСПДн для подключения
к ЗСПД и участие в их прекращении.

2.2 В рамках выполнения основных задач Администратор безопасности осуществляет:

– текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

– текущий контроль технологического процесса автоматизированной обработки информации;

– текущий контроль неизменности состояния СЗИ их параметров и режимов защиты;

– текущий контроль физической сохранности средств и оборудования ИСПДн для подключения к ЗСПД;

– контроль исполнения пользователями установленных в ИСПДн для подключения к ЗСПД правил организации парольной защиты;

– анализ журналов учета событий безопасности СЗИ, с целью выявления возможных нарушений;

– учет машинных носителей информации, используемых в ИСПДн для подключения
к ЗСПД;

– контроль действий пользователей при работе с машинными носителями информации;

– ввод полномочий пользователей в разрешительную систему доступа (матрицу доступа)
и их своевременная корректировка;

– контроль за соблюдением пользователями установленных в ИСПДн для подключения
к ЗСПД правил по организации антивирусного контроля;

– участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности информации;

– контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий
по безопасности информации пользователями ИСПДн для подключения к ЗСПД;

– методическую помощь пользователям ИСПДн для подключения к ЗСПД по вопросам обеспечения безопасности информации и работы с используемыми СЗИ.

3. Обязанности Администратора безопасности информации

Администратор безопасности обязан:

3.1 Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн для подключения
к ЗСПД.

3.2 Участвовать в установке, настройке и сопровождении СЗИ, используемых в ИСПДн для подключения к ЗСПД.

3.3 Вести журнал учета средств защиты информации.

3.4 Участвовать в приемке новых программных средств обработки информации.

3.5 Обеспечить доступ к защищаемой информации пользователям ИСПДн для подключения к ЗСПД согласно их правам доступа, при получении оформленного соответствующим образом разрешения (заявки).

3.6 Уточнять в установленном порядке обязанности пользователей ИСПДн для подключения к ЗСПД при обработке ПДн.

3.7 Вести контроль осуществления резервного копирования информации.

3.8 Анализировать состояние защиты ИСПДн для подключения к ЗСПД.

3.9 Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.10 Контролировать физическую сохранность технических средств обработки информации.

3.11 Контролировать исполнение пользователями ИСПДн для подключения к ЗСПД введенного режима безопасности, а также правильность работы с элементами ИСПДн для подключения к ЗСПД и средствами защиты информации.

3.12 Контролировать исполнение пользователями правил парольной политики.

3.13 Вести контроль над процессом осуществления резервного копирования объектов защиты в ИСПДн для подключения к ЗСПД.

3.14 Еженедельно анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.15 Не допускать установку, использование, хранение и размножение в ИСПДн для подключения к ЗСПД программных средств, не связанных с выполнением функциональных задач.

3.16 Вести контроль за соблюдением установленного в ИСПДн для подключения к ЗСПД порядка организации работы с машинными носителями информации.

3.17 Не допускать к работе на элементах ИСПДн для подключения к ЗСПД посторонних лиц.

3.18 Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) пользователей ИСПДн для подключения к ЗСПД.

3.19 Оказывать помощь пользователям ИСПДн для подключения к ЗСПД в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.20 В случае необходимости информировать руководство о состоянии защиты ИСПДн для подключения к ЗСПД и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.21 В случае отказа работоспособности СЗИ ИСПДн для подключения к ЗСПД принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.22 В случае выявления нарушений режима безопасности ПДн, а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации
их последствий.

3.23 В случае изменения используемых информационных технологий, состава и размещения средств и систем информатики, условий их эксплуатации, которые могут повлиять
на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в «Аттестате соответствия») произвести извещение органа по аттестации, выдавшего «Аттестат соответствия».

3.24 Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки информации, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта не рекомендуется передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. При передачи ремонтным организациям узлов и блоков с элементами накопления и хранения информации, проводится гарантированное уничтожение защищаемой информации с использованием сертифицированных средств защиты от НСД.

4. Права Администратора безопасности

Администратор безопасности имеет право:

4.1 Отключать от ресурсов ИСПДн для подключения к ЗСПД пользователей, осуществивших НСД к защищаемым ресурсам ИСПДн для подключения к ЗСПД для исполнения указания и рекомендации по вопросам ИБ.

4.2 Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИСПДн для подключения к ЗСПД.

4.3 Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн для подключения к ЗСПД при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.4 Осуществлять взаимодействие с руководством и персоналом ИСПДн для подключения к ЗСПД по вопросам обеспечения ИБ.

4.5 Запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.6 Запрашивать и получать от пользователей системы информацию и материалы, необходимые для организации своей работы.

4.7 Вносить на рассмотрение руководства предложения по улучшению состояния безопасности ПДн, обрабатываемых на ИСПДн для подключения к ЗСПД.

4.8 Принимать участие в проведении мероприятий по контролю за обеспечением безопасности персональных данных.

4.9 Вносить изменения в конфигурацию ИСПДн для подключения к ЗСПД и предварительно произведя анализ потенциального воздействия планируемых изменений, согласовав внесение планируемых изменений с должностным лицом (работником), ответственным за обеспечение безопасности ПДн и получив разрешение органа по аттестации, выдавшего «Аттестат соответствия» на ИСПДн для подключения к ЗСПД.

4.10 Действовать в обход установленных процедур идентификации и аутентификации только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5. Действия Администратора безопасности при обнаружении попыток НСД

5.1 К попыткам НСД относятся:

– сеансы работы с телекоммуникационными ресурсами ИСПДн для подключения к ЗСПД незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых, не входят операции доступа к определенным данным или манипулирования ими;

– действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн для подключения к ЗСПД с использованием учетной записи администратора или другого пользователя ИСПДн для подключения к ЗСПД, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

5.2 При выявлении факта/попытки НСД Администратор безопасности обязан:

– прекратить доступ к информационным ресурсам со стороны выявленного участка НСД;

– доложить в случае необходимости ответственному за безопасность и руководителю Учреждения о факте НСД, его результате (успешный, неуспешный) и

предпринятых действиях;

– известить начальника структурного подразделения, в котором работает пользователь,
от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

– проанализировать характер НСД;

– по решению руководства осуществить действия по выяснению причин, приведших к НСД;

– предпринять меры по предотвращению подобных инцидентов в дальнейшем.

6.Ответственность Администратора безопасности

Администраторы безопасности, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального законодательства РФ и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Ответственный за ЗИ Хотов Азамат Лионович

Приложение 3
к приказу № 325 от 03.12.2025г.

Инструкция
администратору 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

1 Общие положения

1.1 Настоящая Инструкция определяет обязанности администратора 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 (далее – ИСПДн для подключения к ЗСПД).

1.2 Администратор ИСПДн для подключения к ЗСПД в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России, регламентирующими документами Учреждения и другими документами в сфере защиты информации.

1.3 Администратор ИСПДн для подключения к ЗСПД подчиняется руководителю Учреждения.

1.4 Методическое руководство работой Администратора ИСПДн для подключения к ЗСПД
в вопросах обеспечения безопасности информации осуществляется ответственным за защиту информации.

1.5 Администратор ИСПДн для подключения к ЗСПД отвечает за обеспечение устойчивой работоспособности программных и аппаратных элементов ИСПДн для подключения к ЗСПД.

1.6 Администратор ИСПДн для подключения к ЗСПД несет персональную ответственность за качество проводимых им работ по обеспечению работоспособности программных и аппаратных элементов ИСПДн для подключения к ЗСПД, в т.ч. за их установку и настройку.

2.Должностные обязанности

Администратор ИСПДн для подключения к ЗСПД обязан:

2.1 Знать и выполнять требования действующих нормативных и руководящих документов,
а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2 Обеспечивать установку, настройку и своевременное обновление элементов автоматизированной системы:

– программного обеспечения автоматизированных рабочих мест (АРМ) (операционные системы, прикладное и специальное программное обеспечение (ПО);

– аппаратных средств;

– аппаратных и программных средств защиты.

2.3 Обеспечивать работоспособность элементов ИСПДн для подключения к ЗСПД и вычислительной сети.

2.4 Осуществлять контроль за порядком учета, создания, хранения и использования

резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5 В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн для подключения к ЗСПД принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.6 Проводить периодический контроль принятых мер по защите, в пределах, возложенных на него функций.

2.7 Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации, в пределах возложенных полномочий.

2.8 Информировать Администратора безопасности ИСПДн для подключения к ЗСПД
о фактах нарушения установленного порядка работ и попытках несанкционированного доступа
к информационным ресурсам ИСПДн для подключения к ЗСПД.

2.9 Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн для подключения к ЗСПД.

2.10 Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

2.11 Присутствовать при выполнении технического обслуживания элементов ИСПДн для подключения к ЗСПД, сторонними физическими людьми и организациями.

2.12 Принимать меры по реагированию, в случае возникновения внештатных ситуаций
и аварийных ситуаций, с целью ликвидации их последствий.

3.Права администратора ИСПДн для подключения к ЗСПД

Администратор ИСПДн для подключения к ЗСПД имеет право:

3.1 Отключать от ресурсов ИСПДн для подключения к ЗСПД пользователей, осуществивших НСД к защищаемым ресурсам ИСПДн для подключения к ЗСПД или нарушивших другие требования по ИБ.

3.2 Давать пользователям обязательные для исполнения указания и рекомендации по вопросам обеспечения нормального функционирования программных и аппаратных элементов ИСПДн для подключения к ЗСПД и локальной вычислительной сети.

3.3 Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн для подключения к ЗСПД при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

3.4 Осуществлять взаимодействие с руководством и персоналом ИСПДн для подключения
к ЗСПД по вопросам нормального функционирования программных и аппаратных элементов ИСПДн для подключения к ЗСПД и локальной вычислительной сети.

3.5 Запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

3.6 Запрашивать и получать от начальников и специалистов структурных подразделений Учреждения информацию и материалы, необходимые для организации своей работы.

3.7 Вносить на рассмотрение руководства предложения по улучшению нормального функционирования программных и аппаратных элементов ИСПДн для подключения к ЗСПД
и локальной вычислительной сети.

3.8 Принимать участие в проведении мероприятий по контролю за обеспечением безопасности персональных данных.

3.9 Действовать в обход установленных процедур идентификации и аутентификации только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

4.Ответственность администратора ИСПДн для подключения к ЗСПД

Администраторы ИСПДн для подключения к ЗСПД, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Ответственный за ЗИ Лакунова Мадина Сафарбиевна

Приложение 4
к приказу № 325 от 03.12.2025г.

Инструкция
о порядке работы пользователя 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 Пользователь осуществляет обработку 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).

1.2 Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации
и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты ИСПДн для подключения к ЗСПД.

1.3 Пользователь несет персональную ответственность за свои действия.

1.4 Пользователь в своей работе руководствуется настоящей инструкцией, нормативными документами ФСТЭК России, ФСБ России, регламентирующими документами Учреждения
и другими документами.

1.5 Методическое руководство работой пользователя в части выполнения положений законодательства Российской Федерации и внутренних документов Учреждения в области обеспечения защиты информации осуществляется администратором безопасности ИСПДн для подключения к ЗСПД.

2 Должностные обязанности

Пользователь информационной системы, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ
к аппаратным средствам, программному обеспечению и данным ИСПДн для подключения к ЗСПД, несет персональную ответственность за свои действия и обязан:

2.1 Решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн для подключения к ЗСПД, присвоенными администратором безопасности данному пользователю. При этом для хранения файлов, содержащих конфиденциальные сведения, разрешается использовать только соответствующим образом учтенные носители информации.

2.2 Знать и выполнять требования, действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

2.3 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.4 Знать и строго выполнять правила работы со средствами защиты информации, установленными на ИСПДн для подключения к ЗСПД.

2.5 Хранить в тайне свой пароль. Периодически менять пароль в соответствии с Инструкцией по организации парольной защиты.

2.6 По окончании работы пользователь обязан произвести стирание остаточной информации на несъемных носителях (жестких дисках) и в оперативной памяти. Одним из способов стирания остаточной информации в оперативной памяти является перезагрузка АРМ.

2.7 В случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля немедленно обратиться к администратору безопасности.

2.8 Строго соблюдать требования Инструкции по организации антивирусной защиты.

В случае обнаружения вирусов немедленно сообщить об этом администратору безопасности.

2.9 Знать и соблюдать установленные требования по учету, хранению машинных носителей информации.

2.10 Немедленно ставить в известность администратора безопасности и в случае подозрения, а также при обнаружении фактов совершения попыток несанкционированного доступа (далее – НСД) к ресурсам ИСПДн для подключения к ЗСПД:

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн для подключения
к ЗСПД;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн для подключения к ЗСПД, выхода из строя или неустойчивого функционирования узлов ИСПДн для подключения к ЗСПД или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– непредусмотренных отводов кабелей и подключенных устройств.

2.11 Для получения консультаций по вопросам работы АРМ и настройке программного обеспечения необходимо обращаться к администратору ИСПДн для подключения к ЗСПД,
по вопросам работы средств защиты информации – к администратору безопасности.

2.12 Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.13 Пользователям ЗАПРЕЩАЕТСЯ:

– использовать компоненты программного и аппаратного обеспечения ИСПДн для подключения к ЗСПД в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн для подключения к ЗСПД или устанавливать дополнительно любые программные и аппаратные средства;

– осуществлять обработку защищаемой информации, в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить защищаемую информацию (содержащую сведения ограниченного распространения), в т.ч. ПДн, на неучтенных носителях информации;

– оставлять включенной без присмотра рабочую станцию (АРМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность администратора безопасности;

– осуществлять какие-либо действия на ИСПДн для подключения к ЗСПД до прохождения процедур идентификации и аутентификации;

– подключать к рабочей станции и вычислительной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– привлекать посторонних лиц для производства ремонта или настройки АРМ;

– разглашать защищаемую информацию третьим лицам;

– копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

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

3 Правила работы в сетях общего доступа и (или) международного информационного обмена

3.1 Работа в сетях общего доступа и (или) международного информационного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн для подключения к ЗСПД, должна проводиться при служебной необходимости.

3.2 При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран и других);

– передавать по Сети защищаемую информацию без использования средств шифрования;

– запрещается скачивать из Сети программное обеспечение и другие файлы;

– запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);

– запрещается нецелевое использование подключения к Сети.

4 Права и ответственность пользователей

Пользователь ИСПДн для подключения к ЗСПД имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями к ресурсам ИСПДн для подключения
к ЗСПД и вверенным ему техническим и программным средствам.

Пользователь ИСПДн для подключения к ЗСПД, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн для подключения к ЗСПД, несет персональную ответственность за свои действия.

Также пользователь ИСПДн для подключения к ЗСПД несет ответственность по действующему законодательству за разглашение сведений конфиденциального характера, ставших известными ему по роду работы.

Пользователи, виновные в несоблюдении настоящей Инструкции, расцениваются как нарушители законодательства РФ в области защиты информации и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Ответственный за ЗИ Лакунова Мадина

Сафарбиевна

Приложение 5
к приказу № 325 от 03.12.2025 г.

Инструкция
по организации парольной защиты 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 Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) при организации доступа на объект 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).

1.2 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей для доступа к ИСПДн для подключения к ЗСПД Учреждения, возлагается на администратора безопасности ИСПДн для подключения к ЗСПД Учреждения (далее – администратор безопасности).

1.3 Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

2 Порядок организации парольной защиты

2.1 Личные пароли должны генерироваться и распределяться централизованно администратором безопасности с учетом следующих требований:

– длина пароля должна быть не менее шести символов, алфавит пароля - не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - от 3 до 10 попыток;

– блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - от 3 до 15 минут;

– в числе символов пароля обязательно должны присутствовать латинские буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

– личный пароль пользователь не имеет права сообщать никому.

2.2 Ответственность за правильность формирования и распределения паролей возлагается на администратора безопасности.

2.3 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 180 дней.

2.4 Блокировка программно-технических средств ИСПДн для подключения к ЗСПД или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации должна составлять от 3 до 15 минут.

2.5 Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.6 В случае прекращения полномочий администратора безопасности производится полная внеплановая смена всех паролей.

2.7 В случае компрометации личного пароля пользователя системы должны быть немедленно предприняты меры в соответствии с п. 2.4 или п. 2.5. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.8 Использование в ИСПДн для подключения к ЗСПД 2-х последних значений паролей при создании новых паролей не допустимо.

2.9 Хранение пользователем значений своих паролей на бумажном носителе допускается только в опечатанном печатью конверте в сейфе у администратора безопасности.

2.10 При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.). Вводимые символы пароля должны отображаться условными знаками «*», «•» или иными знаками.

2.11 Повседневный контроль за действиями исполнителей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

2.12 Временные пароли, заданные при внедрении системы защиты информации ИСПДн для подключения к ЗСПД сотрудниками сторонних организаций, рекомендуется изменить при первом входе в систему.

2.13 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3 Ответственность

3.1 Ответственность за соблюдение требований хранения и использования паролей возлагается на их владельца.

3.2 Ответственность за соблюдение требований, а также за своевременное информирование
о необходимости смены паролей в подразделении возлагается на администратора безопасности ИСПДн для подключения к ЗСПД.

Ответственный за ЗИ Хотов Азамат Лионович

Приложение 6
к приказу № 325 от 03.12.2025г.

Инструкция
о действиях лиц, допущенных к работе 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 Настоящая инструкция определяет действия лиц, допущенных к работе 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 случае возникновения инцидентов в процессах обработки информации, в т. ч. Персональных данных.

1.2 Положения настоящей инструкции обязательны для исполнения всеми должностными лицами, допущенными к работе в ИСПДн для подключения к ЗСПД в части выполнения возложенных на них обязанностей.

1.3. Общими требованиями ко всем лицам, допущенным к работе на ИСПДн для подключения к ЗСПД, в случае возникновения нештатной ситуации или другого инцидента являются:

–лицо, обнаружившее нештатную ситуацию или другой инцидент, немедленно ставит в известность администратора (сетевого или безопасности) ИСПДн для подключения к ЗСПД;

–администратор (сетевой или безопасности) обязан провести анализ ситуации и, в случае невозможности исправить положение, поставить в известность руководство Учреждения. Кроме этого, администратор ИСПДн для подключения к ЗСПД для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей ИСПДн для подключения к ЗСПД;

–по факту возникновения инцидента и выяснению причин его проявления по решению руководства может быть назначена комиссия по реагированию на инциденты ИБ и проведено служебное расследование.

2 Действия пользователей ИСПДн для подключения к ЗСПД при возникновении нештатных ситуаций

2.1 Сбой программного обеспечения.

2.1.1 Администратор ИСПДн для подключения к ЗСПД выясняет причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою.
О произошедшем инциденте администратор ИСПДн для подключения к ЗСПД сообщает руководителю Учреждения для принятия решения, по существу.

2.2 Отключение электропитания технических средств ИСПДн для подключения

к ЗСПД.

2.2.1 Администратор ИСПДн для подключения к ЗСПД проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор ИСПДн для подключения к ЗСПД сообщает руководителю Учреждения для принятия решения, по существу.

2.3 Выход из строя технических средств ИСПДн для подключения к ЗСПД (рабочих станций, источников бесперебойного питания, программно-аппаратных средств межсетевого экранирования и т.д.).

2.3.1 Администратор ИСПДн для подключения к ЗСПД совместно с администратором безопасности ИСПДн для подключения к ЗСПД выполняют мероприятия по ремонту неисправного технического средства ИСПДн для подключения к ЗСПД.

2.3.2 В случае необходимости уведомить о выходе из строя технических средств ИСПДн для подключения к ЗСПД администратора ИСПДн для подключения к ЗСПД.

2.3.3 При необходимости производятся работы по восстановлению программного обеспечения из эталонных копий с составлением акта. О произошедшем инциденте необходимо сообщить администратору безопасности для принятия решения, по существу.

2.4 Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн для подключения к ЗСПД.

2.4.1 При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженную рабочая станцию рекомендуется физически отсоединить от локальной вычислительной сети, и администратор безопасности ИСПДн для подключения к ЗСПД проводит анализ состояния рабочей станции.

2.4.2 После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения из эталонных копий
с составлением акта.

2.4.3 По факту появления ВП в локальной вычислительной сети может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем.

2.5 Утечка информации.

2.5.1 При обнаружении утечки информации ставится в известность администратор безопасности ИСПДн для подключения к ЗСПД. По факту может быть произведена процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн для подключения к ЗСПД и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению
их возникновения.

2.6 Взлом операционной системы средств автоматизации ИСПДн для подключения к ЗСПД (несанкционированное получение доступа к ресурсам операционной системы).

2.6.1. При обнаружении взлома рабочей станции ставятся в известность администратор ИСПДн для подключения к ЗСПД и администратор безопасности ИСПДн для подключения
к ЗСПД.

2.6.2. По возможности производится временное отключение рабочей станции от локальной вычислительной сети ИСПДн для подключения к ЗСПД для проверки на наличие ВП.

2.6.3. Администратором безопасности ИСПДн для подключения к ЗСПД

проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.

2.6.4 В случае необходимости производится восстановление программного обеспечения
из эталонных копий с составлением акта.

2.6.5 По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в ИСПДн для подключения к ЗСПД, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных
на других информационных узлах ИСПДн для подключения к ЗСПД.

2.7 Попытка несанкционированного доступа (НСД).

2.7.1. При попытке НСД администратором безопасности ИСПДн для подключения к ЗСПД проводится анализ ситуации на основе информации журналов регистрации попыток НСД
и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.7.2 Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, администратором ИСПДн для подключения к ЗСПД устанавливаются такие обновления.

2.7.3 По факту попытки НСД может быть проведено служебное расследование. Решение
о необходимости проведения служебного расследования принимается руководителем Учреждения.

2.7.4 В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн для подключения к ЗСПД субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.8 Компрометация ключевой информации (паролей доступа).

2.8.1 При компрометации ключевой информации (пароля доступа) администратором безопасности ИСПДн для подключения к ЗСПД принимаются необходимые меры
по минимизации возможного (или нанесенного) ущерба.

2.8.2 О произошедшем инциденте сообщается руководителю Учреждения для принятия решения, по существу.

2.9 Физическое повреждение или хищение оборудования технических средств ИСПДн для подключения к ЗСПД.

2.9.1 Сотрудником, обнаружившим физическое повреждение элементов ИСПДн для подключения к ЗСПД, ставятся в известность: администратор ИСПДн для подключения к ЗСПД, администратор безопасности ИСПДн для подключения к ЗСПД.

2.9.2 Администратором безопасности ИСПДн для подключения к ЗСПД проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн для подключения к ЗСПД и возможные угрозы информационной безопасности.

2.9.3 О факте повреждения элементов ИСПДн для подключения к ЗСПД в случае необходимости администратор безопасности ИСПДн для подключения к ЗСПД докладывает руководителю Учреждения.

2.9.4 В случае возникновения подозрения на целенаправленный вывод

оборудования
из строя проводится служебное расследование.

2.9.5 Администратором безопасности ИСПДн для подключения к ЗСПД проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.9.6 При необходимости администратором ИСПДн для подключения к ЗСПД проводятся мероприятия по восстановлению программного обеспечения из эталонных копий с составлением акта.

2.10 Невыполнение установленных правил ИБ (правил работы ИСПДн для подключения
к ЗСПД), использование ИСПДн для подключения к ЗСПД с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.10.1 Сотрудником, обнаружившим невыполнение установленных правил ИБ, использование ИСПДн для подключения к ЗСПД с нарушением требований, установленных
в нормативно-технической и (или) конструкторской документации, ставятся в известность администратор безопасности ИСПДн для подключения к ЗСПД.

2.10.2 Администратором безопасности ИСПДн для подключения к ЗСПД проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.10.3 Об обнаруженном факте администратор безопасности ИСПДн для подключения
к ЗСПД в случае необходимости докладывает руководителю Учреждения.

2.10.4 При необходимости по решению руководителя Учреждения по фактам выявленных нарушений проводится служебное расследование.

2.11 Ошибки сотрудников.

2.11.1 В случае возникновения сбоя, связанного с ошибками сотрудников, администратором безопасности ИСПДн для подключения к ЗСПД проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения.

2.11.2 При необходимости проводятся мероприятия по восстановлению программного обеспечения и данных из эталонных копий с составлением акта.

2.11.3 В случае нанесения значительного ущерба вследствие ошибок работников по решению руководства Учреждения может быть проведено служебное расследование.

2.12 Отказ в обслуживании.

2.12.1 Сотрудником, обнаружившим отказ в обслуживании, ставятся в известность администратор безопасности ИСПДн для подключения к ЗСПД.

2.12.2. Администратором безопасности ИСПДн для подключения к ЗСПД проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.12.3 Администратором безопасности ИСПДн для подключения к ЗСПД проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.12.4 При необходимости, проводятся мероприятия по восстановлению программного обеспечения с составлением акта.

2.12.5 О причинах инцидента и принятых мерах администратор безопасности ИСПДн для подключения к ЗСПД в случае необходимости информирует руководителя Учреждения.

2.13 Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн для подключения к ЗСПД.

2.13.1 В случае обнаружения несанкционированного изменения состава программных

и аппаратных средств (конфигурации) ИСПДн для подключения к ЗСПД администратором безопасности ИСПДн для подключения к ЗСПД проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

2.13.2 Администратором ИСПДн для подключения к ЗСПД совместно с администратором безопасности ИСПДн для подключения к ЗСПД проводятся мероприятия по восстановлению программного обеспечения, а также (при необходимости) проверка на наличие компьютерных ВП.

2.13.3 Об инциденте необходимо доложить руководителю Учреждения.

2.14 Техногенные и природные проявления нештатных ситуаций.

2.14.1 При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику, обнаружившему факт возникновения нештатной ситуации:

- немедленно оповестить других сотрудников и принять все меры для самостоятельной оперативной защиты помещения;
- немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
- немедленно сообщить своему администратору АП и администратору безопасности.

2.14.2 После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.14.3 Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

Ответственный за ЗИ Хотов Азамат Лионович

Приложение 7
к приказу № 325 от 03.12.2025г.

Инструкция
по организации резервного копирования 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

Настоящая инструкция определяет действия, связанные с функционированием 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), меры и средства поддержания непрерывности работы и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ИСПДн для подключения к ЗСПД.

Целью настоящего документа является превентивная защита элементов ИСПДн для подключения к ЗСПД от предотвращения потери защищаемой информации.

Задачей данной инструкции является:

-определение мер защиты от потери информации;

-определение действий восстановления в случае потери информации.

Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн для подключения к ЗСПД, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза
в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие
к потере защищаемой информации, назначается администратор безопасности ИСПДн для подключения к ЗСПД.

2 Порядок организации резервного копирования в ИСПДн для подключения к ЗСПД

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн для подключения к ЗСПД в случае возникновения аварийной ситуации, повлекшей
за собой повреждение или утрату данных.

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемой информации – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн для подключения к ЗСПД – не реже раза
в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Резервному копированию подлежит информация следующих основных категорий:
- персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;
- информация, обрабатываемая пользователями в ИСПДн для подключения к ЗСПД, а также информация, необходимая для восстановления работоспособности ИСПДн для подключения к ЗСПД, в т.ч. систем управления базами данных (СУБД) общего пользования
и справочно-информационные системы общего использования;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн для подключения к ЗСПД;
- регистрационная информация системы информационной безопасности ИСПДн для подключения к ЗСПД;
- другая информация ИСПДн для подключения к ЗСПД, по мнению пользователей и администраторов, являющаяся критичной для работоспособности ИСПДн для подключения
к ЗСПД.

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Машинные носители информации, на которые произведено резервное копирование, должны быть учтены в журнале учета машинных носителей для архивного копирования (Приложение 2), который находится у администратора безопасности. В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

Физический доступ к архивным копиям предоставляется только администратору ИСПДн для подключения к ЗСПД и администратору безопасности.

Передача машинных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

Уничтожение отделяемых машинных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

В случае необходимости восстановление данных из резервных копий производится администратором ИСПДн для подключения к ЗСПД или администратором безопасности.

Восстановление данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

3 Ответственность

Ответственность за контроль над своевременным осуществлением резервного копирования
и соблюдением настоящей инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности ИСПДн для подключения к ЗСПД.

Ответственный за ЗИ Хотов Азамат Лионович

Приложение 8
к приказу № 325 от 03.12.2025г.

Инструкция
по защите информации о событиях безопасности 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

Настоящая инструкция по организации защиты информации о событиях безопасности
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 основные мероприятия по защите информации о событиях безопасности в ИСПДн для подключения к ЗСПД.

2 Основные мероприятия по защите информации о событиях безопасности

События безопасности, подлежащие регистрации в ИСПДн для подключения к ЗСПД, определяются с учетом способов реализации угроз безопасности информации. К событиям безопасности, подлежащим регистрации в ИСПДн для подключения к ЗСПД, отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИСПДн для подключения к ЗСПД, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также нарушения штатного функционирования средств защиты информации.

В ИСПДн для подключения к ЗСПД определены следующие события безопасности, подлежащие регистрации:

1. События, связанные с регистрацией входа (выхода) субъектов доступа в систему
и загрузки операционной системы. Состав и содержание информации включают дату и время входа (выхода) в систему (из системы) или загрузки операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.
2. События, связанные с регистрацией подключения машинных носителей информации
и вывода информации на носители информации. Состав и содержание регистрационных записей включает: дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.
3. События, связанные с регистрацией запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации. Состав и содержание регистрационных записей включает: дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта

доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4. События, связанные с регистрацией попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Состав и содержание регистрационных записей включает: дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

5. События, связанные с регистрацией попыток доступа программных средств
к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей). Состав
и содержание информации должны включать: дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер)).

6. События, связанные с изменением привилегий учетных записей.

7. События, связанные с регистрацией запланированного обновления антивирусных баз. Состав и содержание информации должны включать дату и время обновления.

8. События, связанные с регистрацией запланированного обновления ОС (ведется в штатных журналах ОС). Состав и содержание информации должны, включать дату и время обновления, состав обновления.

События безопасности, подлежащие регистрации ИСПДн для подключения к ЗСПД, и сроки хранения соответствующих записей регистрационных журналов, обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн для подключения
к ЗСПД.

Так же подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИСПДн для подключения к ЗСПД.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется администратором безопасности, исходя из возможностей реализации угроз безопасности информации.

Срок хранения информации о зарегистрированных событиях безопасности должен составлять не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с методическими документами, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору безопасности ИСПДн для подключения к ЗСПД.

В ИСПДн для подключения к ЗСПД для обеспечения защиты информации о событиях безопасности, перед установкой СЗИ осуществляется синхронизация системного времени и даты. Администратор безопасности осуществляет контроль неизменности установленного системного времени и проводит периодическую проверку журналов регистрации событий, для контроля правильности отображения временных меток.

Сбор, запись и хранение информации о событиях безопасности осуществляется с помощью встроенных средств операционной системы и установленных СЗИ.

В целях предотвращения сбоев при регистрации событий безопасности СЗИ и операционной системы в ИСПДн для подключения к ЗСПД:

1. Администратору безопасности необходимо еженедельно проверять журналы истрации событий СЗИ и операционной системы на наполненность и, в случае необходимости, оизводить их архивацию.
2. Увеличить при необходимости объем, выделяемой под журналы событий опасности СЗИ и операционной системы памяти.
3. Включить автоматическую перезапись новых событий безопасности поверх аревших для предотвращения возникновения ошибок переполнения журналов.
4. Настройки прав учетных записей пользователей ИСПДн для подключения СПД должны исключать возможность внесения пользователями изменений в журналы событий опасности, настройки СЗИ и операционной системы.
5. При появлении в ИСПДн для подключения к ЗСПД ошибок операционной системы или СЗИ пользователю необходимо уведомить администратора безопасности и приостановить работу до устранения ошибки.

Ответственный за ЗИ Шуляк Александр Борисов

Приложение 9
к приказу № 325 от 03.12.2025г.

Инструкция
о порядке изменения состава и конфигурации технических и программных средств 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

Настоящей инструкцией регламентируется порядок проведения модификации программного обеспечения и технического обслуживания средств вычислительной техники 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).

Право внесения изменений в конфигурацию программно-аппаратных средств информационных узлов (рабочих станций, серверов) и телекоммуникационного оборудования, предназначенного для обработки информации в ИСПДн для подключения к ЗСПД, предоставляется:

– в отношении системных и прикладных программных средств, а также в отношении аппаратных средств ИСПДн для подключения к ЗСПД и программно-аппаратных средств телекоммуникаций – администратору ИСПДн для подключения к ЗСПД;

– в отношении программно-аппаратных и программных СЗИ - администратору безопасности.

Изменение конфигурации аппаратно-программных средств защищенных рабочих станций (АРМ) и серверов кем-либо, кроме перечисленных лиц, запрещено.

2 Порядок внесения изменений в конфигурацию программных и аппаратных средств ИСПДн для подключения к ЗСПД

Для внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций ИСПДн для подключения к ЗСПД начальнику структурного подразделения, в котором вносятся изменения, подается заявка на имя администратора безопасности, которая им рассматривается.

В заявках могут быть указаны следующие виды необходимых изменений в составе программных и аппаратных средств рабочих станций и серверов подразделения:

– установка в подразделении новой рабочей станции (АРМ) или сервера;

– замена рабочей станции (АРМ) или сервера подразделения;

– изъятие рабочей станции (АРМ) или сервера подразделения;

– добавление устройства (узла, блока) в состав конкретной рабочей станции (АРМ) или сервера подразделения;

– замена устройства (узла, блока) в составе конкретной рабочей станции (АРМ) или сервера подразделения;

– изъятие устройства (узла, блока) из состава конкретной рабочей станции (АРМ) или сервера;

– установка (развертывание) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной

задачи (добавление возможности решения данной задачи на данной рабочей станции или сервере);

– обновление (замена) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

– удаление с конкретной рабочей станции (АРМ) или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной рабочей станции).

В заявке указываются условные наименования развернутых рабочих станций (АРМ) и серверов в соответствии с их паспортами. Программные средства указываются в соответствии
с перечнем программных средств и программ, которые используются в ИСПДн для подключения к ЗСПД.

Администратор безопасности при согласовании заявки учитывает возможность совмещения решения новых задач (обработки информации) на указанных в заявке рабочих станциях (АРМ) или серверах в соответствии с требованиями по безопасности.

Все изменения в конфигурации технических и программных средств ИСПДн для подключения к ЗСПД должны производиться только после их согласования с органом по аттестации, выдавшим «Аттестат соответствия» на ИСПДн для подключения к ЗСПД.

После этого осуществляется непосредственное исполнение работ по внесению изменений
в конфигурацию рабочих станций (АРМ) или серверов ИСПДн для подключения к ЗСПД.

Начальник структурного подразделения, в котором установлены аппаратно-программные средства, подлежащие модернизации, допускает уполномоченных исполнителей (администратора ИСПДн для подключения к ЗСПД и (или) администратора безопасности) к внесению изменений
в состав аппаратных средств и ПО.

Установка, изменение (обновление) и удаление системных и прикладных программных средств производится администратором ИСПДн для подключения к ЗСПД.

Установка, снятие и внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов на рабочих станциях осуществляется администратором безопасности. Работы производятся в присутствии пользователя данной рабочей станции.

Установка или обновление подсистем ИСПДн для подключения к ЗСПД проводится в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Модификация ПО на сервере осуществляется администратором ИСПДн для подключения
к ЗСПД по согласованию с администратором безопасности.

После установки модифицированных модулей на сервер администратор безопасности устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм
с помощью специальных программных средств, прошедших оценку соответствия).

После проведения модификации ПО на рабочих станциях администратором безопасности должен быть проведен антивирусный контроль.

Установка и обновление общесистемного и прикладного ПО на рабочие станции (АРМ)
и серверы производится с оригинальных лицензионных дистрибутивных носителей (компакт-дисков и др.), полученных установленным порядком.

Все добавляемые программные и аппаратные компоненты предварительно

проверяются
на работоспособность, контроль наличия проверок работоспособности осуществляет администратор ИСПДн для подключения к ЗСПД.

После установки (обновления) ПО, администратор ИСПДн для подключения к ЗСПД (при использовании специализированных СЗИ от НСД - администратор безопасности) производит настройку средств управления доступом к данному программному средству и проверяет работоспособность ПО и правильность настройки СЗИ.

После завершения работ по внесению изменений в состав аппаратных средств рабочей станции (АРМ), ее системный блок закрывается уполномоченным работником подразделения ИТ на ключ (при наличии штатных механических замков) и опечатывается (пломбируется, защищается специальной наклейкой) с возможностью постоянного визуального контроля
за ее целостностью.

Уполномоченные исполнители работ производят соответствующую запись в журнале фактов вскрытия и опечатывания рабочих станций (серверов), выполнения профилактических работ, установки и модификации аппаратных и программных средств рабочих станций (серверов) ИСПДн для подключения к ЗСПД (Приложение 1).

Администратор безопасности проводит периодический контроль за опечатыванием узлов
и блоков ИСПДн для подключения к ЗСПД.

На обратной стороне заявки (Приложение 2) делается отметка о выполнении, и исполненная заявка передается администратору безопасности для хранения.

При изъятии рабочей станции (сервера) из состава ИСПДн для подключения к ЗСПД,
ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как с данной рабочей станции (сервера) будут удалены все СЗИ и предприняты необходимые меры для затирания (удаления) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом об уничтожении информации, хранившейся на диске компьютера.

Ответственный за ЗИ Хотов Азамат Лионович

Приложение 1
к Инструкции о порядке изменения состава и конфигурации
технических и программных средств ИСПДн для подключения к ЗСПД

(форма)

Журнал фактов вскрытия и опечатывания рабочих станций и серверов, выполнения профилактических работ, установки и модификации программных средств на элементах 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

Начат «____» _____ 20__ г.

Окончен «____» _____ 20__ г.

На _____листах

_____ _____

должность и Ф.И.О. ответственного за ведение и хранение журнала Подпись

№ п/п	Дата	Краткое описание выполненной работы	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию АРМ, подпись	Подпись Администратора безопасности	Примечание (ссылка на заявку)

Приложение 2
к Инструкции о порядке изменения состава и конфигурации технических и программных средств ИСПДн для подключения к ЗСПД

(форма)

Администратору безопасности информации
ИСПДн для подключения к ЗСПД

ЗАЯВКА

на внесение изменений в состав аппаратно-программных/программных средств ИСПДн для подключения к ЗСПД

Прошу произвести следующие изменения конфигурации аппаратно-программных/программных средств ИСПДн для подключения к ЗСПД в

_____
___

(наименование подразделения)

развернуть новую рабочую станцию, установить на (обновить на / снять с) нее _____ компоненты, необходимые для решения следующих задач:

_____
___

(наименование задач)

Начальник _____

(наименование подразделения)

«___» _____ 20__ г. _____ _____

(подпись) (фамилия и инициалы)

Отметка о выполнении:

_____ _____

(фамилия, инициалы) (подпись)

«_____» _____

Приложение 10
к приказу № 325 от 03.12.2025г.

Инструкция
по обеспечению защиты информации при выводе из эксплуатации или после принятия решения об окончании обработки информации 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. Настоящая инструкция предназначена для обеспечения защиты информации при выводе из эксплуатации или после принятия решения об окончании обработки информации 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).

2 Порядок организации

2.1. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором ИСПДн для подключения к ЗСПД, в соответствии
с эксплуатационной документацией на систему защиты информации ИСПДн для подключения
к ЗСПД и организационно-распорядительными документами по защите информации, и в том числе включает:
- архивирование информации, содержащейся в информационной системе;
- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2.2. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора ИСПДн для подключения к ЗСПД.

2.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации на ИСПДн для подключения к ЗСПД, производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или
в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется гарантированная очистка (стирание) данных
с этих машинных носителей информации в соответствии с утвержденным Порядком обращения, хранения и уничтожения машинных носителей защищаемой информации в ИСПДн для подключения к ЗСПД.

При выводе из эксплуатации элементов ИСПДн для подключения к ЗСПД, содержащих оптические носители информации (CD-дисков), используемые для хранения и обработки информации, осуществляется физическое уничтожение этих оптических

носителей информации в соответствии с утвержденным порядком обращения, хранения и уничтожения машинных носителей информации в ИСПДн для подключения к ЗСПД.

3 Ответственность

3.1 Ответственность за соблюдение требований по обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения
об окончании обработки информации возлагается на оператора.

Ответственный за ЗИ Хотов Азамат Лионович

Приложение 11
к приказу № 325 от 03.12.2025г.

Инструкция
Об использовании мобильных технических средств 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

Настоящая инструкция определяет порядок использования мобильных технических средств 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 качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

При использовании мобильных технических средств в ИСПДн для подключения к ЗСПД запрещается:

1. Обрабатывать защищаемую информацию на ноутбуках, используемых в качестве ОТСС за пределами контролируемой зоны;

2. Выносить за пределами контролируемой зоны ноутбуки, используемые в качестве ОТСС, кроме случаев передачи в ремонт;

3. Использовать мобильные технические средства ИСПДн для подключения к ЗСПД
в целях, не связанных с обработкой защищаемой информацией в том числе ПДн;

4. Использовать в ИСПДн для подключения к ЗСПД съемные машинные носители информации, не зарегистрированные в журнале учета съемных носителей информации;

5. Подключение к элементам ИСПДн для подключения к ЗСПД, внешних устройств,
не входящих в его состав (мобильных телефонов, цифровых фотоаппаратов, адаптеров беспроводной связи и иных).

6. Использовать в ИСПДн для подключения к ЗСПД беспроводные сети (WiFi, Bluetooth
и др.);

7. Хранение на мобильных технических средствах ИСПДн для подключения к ЗСПД личной информации, а также информации, не имеющей отношения к служебной деятельности (музыкальные файлы, фоновые изображения и прочее).

Устройства ввода аудио (микрофоны) и видео (веб камеры) информации мобильных технических средств, используемых в ИСПДн для подключения к ЗСПД, должны быть отключены.

Администратором безопасности ИСПДн для подключения к ЗСПД обеспечивается:

Запрет использования в информационной системе, не входящих в ее состав (находящихся
в личном использовании) съемных машинных носителей информации;

Запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация,

ответственные
за принятие мер защиты информации);

Очистка машинного носителя информации мобильного технического средства, переустановка программного обеспечения и выполнение иных мер по защите информации мобильных технических средств, после их использования за пределами контролируемой зоны;

Предоставление доступа с использованием мобильных технических средств к объектам доступа информационной системы только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

Запрет использования устройств ввода аудио (микрофоны) и видео (веб-камеры) информации технических средств;

Подключение мобильных технических средств к ресурсам ИСПДн для подключения
к ЗСПД должно осуществляться только по проводным каналам связи. Использование для подключения к ресурсам ИСПДн для подключения к ЗСПД беспроводных точек доступа (Wi-Fi
и др.) запрещено.

Администратором безопасности ИСПДн для подключения к ЗСПД обеспечивается запрет подключения к беспроводным сетям доступа технических средств, имеющих в своем составе модули беспроводного доступа (моноблоки, стационарные АРМ, принтера и другие технические средства).

Ответственность за правильную эксплуатацию мобильных и технических средств, имеющих в своем составе модули беспроводного доступа, несут пользователи ИСПДн для подключения к ЗСПД и Администратор безопасности ИСПДн для подключения к ЗСПД.

Контроль за соблюдением пользователями правил эксплуатации мобильных технических средств и технических средств, имеющих в своем составе модули беспроводного доступа, возлагается на Администратора безопасности ИСПДн для подключения к ЗСПД.

Контроль за соблюдением пользователями правил эксплуатации мобильных технических средств возлагается на администратора безопасности ИСПДн для подключения к ЗСПД.

Ответственный за ЗИ Хотов Азамат Лионович

Приложение 12
к приказу № 325 от 03.12.2025г.

Инструкция
по организации антивирусной защиты 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 требования

1.1 Настоящая инструкция определяет требования к организации антивирусной защиты
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) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность персонала ИСПДн для подключения к ЗСПД, осуществляющего эксплуатацию и сопровождение ИСПДн для подключения к ЗСПД за их выполнение.

1.2 К использованию в ИСПДн для подключения к ЗСПД допускаются только лицензионные и сертифицированные ФСТЭК России средства антивирусной защиты, закупленные у разработчиков (поставщиков) указанных средств.

1.3 Установка и настройка средств антивирусной защиты, а также обновление антивирусных баз на АРМ пользователей и серверах ИСПДн для подключения к ЗСПД, осуществляется Администратором безопасности ИСПДн для подключения к ЗСПД в соответствии
с руководствами по применению конкретных антивирусных средств.

1.4 Средства антивирусной защиты должны быть установлены на все средства вычислительной техники (далее по тексту - СВТ) (при наличии технической возможности), входящие в состав ИСПДн для подключения к ЗСПД.

1.5 В ИСПДн для подключения к ЗСПД права по управлению (администрированию) средствами антивирусной защиты предоставлены только Администратору безопасности ИСПДн для подключения к ЗСПД.

1.6 Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется Ответственным за организацию и обеспечение защиты информации ИСПДн для подключения к ЗСПД с привлечением (при необходимости) Администратора безопасности ИСПДн для подключения к ЗСПД и/или специалистов лицензированной организации.

1.7 Должностные лица, допущенные к работе в ИСПДн для подключения к ЗСПД, не должны допускать использования в ИСПДн для подключения к ЗСПД программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

1.8 В ИСПДн для подключения к ЗСПД обеспечивается централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (автоматизированных рабочих местах и серверах).

1.9 В ИСПДн для подключения к ЗСПД обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

1.10 Администратор безопасности ИСПДн для подключения к ЗСПД обеспечивает

получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

1.11 Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с сервера обновлений производителя антивирусного средства.

1.12 В виртуальной инфраструктуре (при ее наличии) обеспечивается реализация и управление антивирусной защитой:

- проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;
- проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

2 Применение средств антивирусной защиты

2.1 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), Администратором безопасности ИСПДн для подключения к ЗСПД должна быть выполнена антивирусная проверка.

2.2 При загрузке АРМ и серверов средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

2.3 Антивирусный контроль всех дисков и файлов АРМ пользователей ИСПДн для подключения к ЗСПД, должен проводиться регулярно (но не реже 1 раза в неделю) в автоматическом режиме в соответствии с установленным расписанием.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.4 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.5 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан поставить в известность Администратора безопасности ИСПДн для подключения к ЗСПД, который обязан в таком случае провести внеочередной антивирусной контроль.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов Администратор безопасности ИСПДн для подключения к ЗСПД обязан:

- приостановить работу в ИСПДн для подключения к ЗСПД;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов.

2.6 Администратор безопасности ИСПДн для подключения к ЗСПД проводит лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы
и после этого вновь проводит антивирусный контроль.

2.7 В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, Администратор безопасности ИСПДн для подключения к ЗСПД обязан запретить работу в ИСПДн для подключения к ЗСПД, поставить в известность Ответственного за организацию обработки и обеспечение защиты информации и в возможно короткие сроки обновить пакет антивирусных программ.

3 Ответственность при организации антивирусной защиты

3.1 Ответственность за организацию антивирусной защиты ИСПДн для подключения
к ЗСПД в соответствии с требованиями настоящей Инструкции возлагается на Администратора безопасности ИСПДн для подключения к ЗСПД.

3.2 Периодический контроль за состоянием антивирусной защиты в ИСПДн для подключения к ЗСПД, а также за соблюдением установленного порядка антивирусного контроля
и выполнением требований настоящей Инструкции осуществляется Администратором безопасности ИСПДн для подключения к ЗСПД.

3.3 Пользователи ИСПДн для подключения к ЗСПД обязаны соблюдать требования настоящей Инструкции и должны быть ознакомлены с настоящей Инструкцией под роспись.

Ответственный за ЗИ Хотов Азамат Лионович

Лист ознакомления с приказом № 325 от 03.12.2025г.

«Об утверждении инструкций 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

Ф.И.О.	Должность	Роль в ИСПДн	Подпись, дата