КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ ФИНАНСХЭМКІЭ И МИНИСТЕРСТВЭ
КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ ФИНАНСЛА МИНИСТЕРСТВОСУ
МИНИСТЕРСТВО ФИНАНСОВ
КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ
(МИНФИН КБР)

ПРИКАЗ

« 12» февраля 20 20 г. г. Нальчик № 20

О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПРИКАЗ МИНИСТЕРСТВА ФИНАНСОВ КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ «О МЕРАХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МИНИСТЕРСТВЕ ФИНАНСОВ КБР»

П р и к а з ы в а ю:

1. Внести в приказ Министерства финансов КБР от 17.03.2016 г. № 29 «О мерах по обеспечению информационной безопасности в Министерстве финансов КБР» следующие изменения:

- пункт 3.2 раздела 3. «Проведение резервного копирования» Инструкции по резервному копированию, архивированию и восстановлению информации в автоматизированных системах Министерства финансов Кабардино – Балкарской Республики дополнить пунктом следующего содержания:

«3. Факт создания квартальных копий БД необходимо фиксировать в Журнале учета резервного копирования и восстановления данных Министерства финансов Кабардино-Балкарской Республики.» (Приложение №1).

2. Утвердить Журнал учета резервного копирования и восстановления данных Министерства финансов Кабардино-Балкарской Республики согласно приложению 1 к настоящему приказу.

3. Инструкцию о системе паролирования в Министерстве финансов Кабардино – Балкарской Республики дополнить пунктами следующего содержания:

«2.1. Смену логина и пароля пользователи регистрируют в Журнале регистрации паролей пользователей согласно приложению 2.

2.2. При технологической необходимости смены паролей некоторых работников (исполнителей), в том числе в их отсутствие (в случае возникновения внештатных ситуаций), все изменения вносятся в Журнал регистрации паролей пользователей.

2.3. Контроль за сменой паролей пользователей осуществляется администратором безопасности информационных систем персональных данных Министерства финансов КБР.

11. 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.).

12. Запрещается записывать пароли на бумаге, в файле, в электронной записной книжке и других носителях информации.

13. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.».

4. Утвердить Журнал регистрации паролей пользователей Министерства финансов Кабардино-Балкарской Республики согласно приложению 2 к настоящему приказу.

5. Дополнить пунктом 5.1. следующего содержания:

«5.1. Утвердить Инструкцию по учёту, хранению и уничтожению машинных носителей персональных данных в Министерстве финансов Кабардино-Балкарской Республики»;

6. Дополнить пунктом 5.2. следующего содержания:

«5.2. Утвердить Инструкцию пользователя по обеспечению информационной безопасности при работе с персональными данными Министерства финансов Кабардино-Балкарской Республики».

7. Утвердить Инструкцию по учёту, хранению и уничтожению машинных носителей персональных данных в Министерстве финансов Кабардино-Балкарской Республики согласно приложению 3 к настоящему приказу.

8. Утвердить Инструкцию пользователя по обеспечению информационной безопасности при работе с персональными данными Министерства финансов Кабардино-Балкарской Республики, согласно приложению 4 к настоящему приказу.

9. Признать утратившим силу пункт 2 и Инструкцию учёта машинных носителей, содержащих конфиденциальную информацию в Министерстве

финансов КБР, утвержденные приказом Министерства финансов КБР от 17.03.2016 г. № 29 «О мерах по обеспечению информационной безопасности в Министерстве финансов КБР».

10. Контроль за исполнением настоящего приказа возложить на заместителя министра финансов КБР Калабекова А.М.

И.о. министра финансов КБР Е.А. Лисун

Приложение 1
к приказу Минфина КБР
«____» _____ 20____г № ____

Журнал учета резервного копирования и восстановления данных Министерства финансов Кабардино-Балкарской Республики

Дата проведения резервного копирования/восстановления	Наименование резервной копии	Наименование информационной системы/базы данных	Ф.И.О., подпись ответственного	Тип носителя/регистрационный номер машинного носителя	Ф.И.О., подпись ответственного за хранение	Примечание

Приложение 2
к приказу Минфина КБР
«____» _____ 20____г № ____

Журнал регистрации паролей пользователей Министерства финансов Кабардино-Балкарской Республики

№ п/п	Наименование отдела	Фамилия, имя, отчество	Имя пользователя	Пароль (6 символов)	Срок действия пароля		Контроль о смене пароля	
					Дата смены пароля	Дата окончания действия	Подпись администратора безопасности ИС Пд	Дата проверки

Приложение 4
к приказу Министерства финансов КБР
от «___» _____ 20__ г. № ___

ИНСТРУКЦИЯ
пользователя по обеспечению информационной безопасности при работе с персональными данными Министерства финансов Кабардино-Балкарской Республики

1. Общее положения

Настоящая Инструкция разработана в целях регламентации действий пользователей по обеспечению информационной безопасности при работе с персональными данными, при их обработке в информационных системах в Министерстве финансов КБР, и определяет:

- меры обеспечения безопасности информации и правила работы с информацией ограниченного доступа;
- правила при работе с ресурсами сети Интернет и электронной почтой;
- возможные аварийные ситуации, меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем персональных данных (далее – ИСПДн) после аварийных ситуаций.

Задачей данной Инструкции является:

- определение мер защиты ИСПДн от нарушения (прекращения) работоспособности;
- определение действий по восстановлению ИСПДн в случае нарушения (прекращения) работоспособности.

Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, 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.

Перед началом эксплуатации автоматизированного рабочего места

пользователь должен ознакомиться:

– с положениями настоящего документа;

– с регламентирующими документами по обеспечению информационной безопасности, принятыми в Министерстве финансов Кабардино-Балкарской Республики;

– с руководствами пользователя по эксплуатации информационных систем, к которым пользователю предоставлен доступ.

2. Обязанности пользователя

Пользователем информационной системы (далее – Пользователь) является лицо, участвующее в процессах автоматизированной обработки информации в информационной системе и имеющее доступ к программному обеспечению и данным, обрабатываемым в этой системе.

Каждый Пользователь несет персональную ответственность за свои действия и обязан:

–знать и строго соблюдать установленные настоящей Инструкцией правила обеспечения безопасности информации при работе с программными средствами и средствами защиты информации в информационных;

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

–обеспечивать запирание помещения на ключ при выходе всех работников из помещения, в котором осуществляется работа с информационными системами;

– поддерживать постоянную работу (не отключать (блокировать) средства защиты информации);

– сообщать ответственному за эксплуатацию информационных систем (инженеру по автоматизации, технику) о замеченных нарушениях информационной безопасности (в т. ч. о сбоях в работе средств защиты информации);

–передавать в случае прекращения трудовых отношений Ответственному за организацию обработки персональных данных в Министерстве финансов Кабардино-Балкарской Республики все имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного доступа.

3. Правила работы с информацией ограниченного доступа

в информационных системах

При работе с информацией ограниченного доступа пользователю запрещается:

– создавать и хранить документы, содержащие информацию ограниченного доступа, в папках, предназначенных для обмена открытыми документами;

– работать с информацией ограниченного доступа в общественных местах и на рабочих станциях, не оборудованных средствами защиты информации;

– осуществлять обработку информации на автоматизированном рабочем месте в присутствии лиц, не допущенных к данной информации;

– оставлять без личного контроля съемные и другие носители информации (в т. ч. и установленные на автоматизированном рабочем месте), распечатки, содержащие информацию ограниченного доступа;

– записывать на устройства, предназначенные для хранения информации ограниченного доступа, посторонние данные;

– использовать информацию ограниченного доступа в личных целях, в т. ч. в целях получения выгоды;

– выносить за пределы Министерства финансов Кабардино-Балкарской Республики материальные носители с информацией ограниченного доступа;

– оставлять без личного контроля включенное автоматизированное рабочее место без активированной блокировки.

4. Процедура блокирования доступа к автоматизированному рабочему месту

При необходимости временно прервать работу на автоматизированном рабочем месте, для защиты от несанкционированного использования необходимо воспользоваться функцией временной блокировки компьютера, при которой блокируется клавиатура и экран монитора.

Порядок действий при блокировке автоматизированного рабочего места вручную: нажать комбинацию клавиш «Win» (между клавишами «Ctrl» и «Alt») + «L».

Для разблокировки автоматизированного рабочего места пользователю необходимо ввести свой пароль доступа.

5. Правила обращения со съемными носителями

Пользователь использует съемные носители информации только в случаях, когда это необходимо для выполнения трудовых (служебных) обязанностей. При использовании съемных носителей Пользователь обязан:

– использовать съемные носители исключительно для выполнения служебных обязанностей и не использовать в личных целях;

– обеспечивать физическую безопасность съемных носителей;

– обеспечивать проверку отсутствия вредоносного программного обеспечения на съемных носителях;

– извещать о фактах утери съемных носителей, содержавших персональные данные работников;

– не передавать съемные носители третьим лицам при отсутствии в этом производственной необходимости;

– не оставлять съемные носители без присмотра.

6. Использование электронной почты и ресурсов сети Интернет

При использовании электронной почты Пользователям запрещается:

– пересылать информацию ограниченного доступа с использованием общедоступных почтовых сервисов (Яндекс, Рамблер, Mail.ru, Google и другие);

– открывать вложения подозрительных электронных сообщений: сообщений от незнакомых отправителей; сообщений, содержащих исполняемые файлы (EXE, COM, BAT); сообщений рекламного, развлекательного, оскорбительного характера;

– переходить по ссылкам на сайты из подозрительных электронных сообщений, в том числе сообщений, содержащих приглашения «открыть», «запустить», «посетить», «нажать», «перейти»;

– отправлять электронные письма от имени других работников Министерства финансов Кабардино-Балкарской Республики, если иное не определено их служебными обязанностями;

– предпринимать попытки несанкционированного доступа к почтовым ящикам других работников Министерства финансов Кабардино-Балкарской Республики.

При использовании ресурсов сети Интернет Пользователям запрещается:

– использовать для обмена информацией ограниченного доступа сайты, предоставляющие услуги хранения и обмена информацией;

– размещать, публиковать информацию ограниченного доступа на

общедоступных ресурсах;

–загружать из сети Интернет программное обеспечение и устанавливать его на автоматизированные рабочие места.

7. Порядок реагирования сотрудников на аварийную ситуацию

7.1. Действия при возникновении аварийной ситуации

Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в таблице.

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо

16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телекоммуникационные и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физически разрыв внешних каналов связи

В кратчайшие сроки, ответственными сотрудниками (Администратор информационной безопасности ПД, ответственный за организацию обработки ПД) предпринимают меры по восстановлению работоспособности.

Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

Ответственные сотрудники (Администратор информационной безопасности ПД, ответственный за организацию обработки ПД) ознакамливают всех сотрудников Министерства финансов Кабардино-Балкарской Республики, находящихся в их зоне ответственности, с данной инструкцией под роспись в Журнале ознакомления сотрудников с требованиями законодательства РФ и КБР о персональных данных.

8. Ответственность пользователя

Пользователь несет персональную ответственность за надлежащее исполнение своих обязанностей, а также сохранность технических средств автоматизированного рабочего места, съемных носителей информации, электронных идентификаторов и целостность установленного программного обеспечения.

Приложение 3
к приказу Министерства финансов КБР
от «_____» _____ 20____ г. № _____

ИНСТРУКЦИЯ
ПО УЧЁТУ, ХРАНЕНИЮ И УНИЧТОЖЕНИЮ МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ФИНАНСОВ КБР

1. Общие положения

Настоящая инструкция разработана в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Целью данной Инструкции является определение правил по учету, хранению и уничтожению машинных носителей персональных данных (далее – ПДн) в Министерстве финансов Кабардино-балкарской Республики.

В настоящей Инструкции использованы следующие термины:

а) информационная система персональных данных (ИСПДн);

б) автоматизированное рабочее место (АРМ) – персональный компьютер с прикладным программным обеспечением, используемый для выполнения установленной трудовой функции работника;

в) администратор информационной системы (АИС) - технический специалист, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники;

г) вредоносное программное обеспечение - программное обеспечение или изменения в программное обеспечение, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации;

д) информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации;

е) машинный носитель информации - материальный носитель, используемый для хранения и передачи электронной информации.

2. Учет, хранение и обращение с машинными носителями

2.1. Все находящиеся на хранении и в обращении машинные носители подлежат учёту.

2.2. Каждый машинный носитель должен иметь маркировку с уникальным учётным номером.

2.3. Учет и выдачу машинных носителей осуществляет администратор информационной безопасности Министерства финансов КБР. Факт выдачи машинного носителя пользователю фиксируется в Журнале учета выдачи машинных носителей персональных данных в Министерстве финансов КБР.

2.4. При использовании машинных носителей необходимо:

а) соблюдать требования настоящей рабочей инструкции;

б) использовать машинные носители исключительно для выполнения своих должностных обязанностей;

в) информировать администраторов ИС о любых фактах нарушения требований настоящей Инструкции;

г) бережно относиться к машинным носителям;

д) обеспечивать физическую безопасность машинных носителей;

е) извещать администраторов ИС о фактах утраты (кражи) машинных носителей.

2.5. При использовании машинных носителей запрещается:

а) использовать машинные носители в личных целях;

б) передавать машинные носители другим лицам (кроме администратора безопасности информационных систем ПДн);

в) хранить машинные носители вместе с общедоступными данными, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

г) выносить носители из служебных помещений для работы с ними на дому (за исключением служебной необходимости) и т. д.

2.6. Администратор ИС имеет право блокировать или ограничивать использование машинных носителей, изымать, хранить машинные носители в случае увольнения или перевода работника в другое структурное подразделение.

2.7. Информация, хранящаяся на машинных носителях, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

2.8. В случае утраты или уничтожения машинных носителей либо разглашении содержащихся в них сведений, работник установивший факт

утраты/разглашения обязан немедленно сообщить об этом начальнику отдела информационных технологий. В журнале учета выдачи машинных носителей персональных данных в Министерстве финансов КБР (Приложение №1) вносятся соответствующие отметки об утрате или уничтожении машинных носителей персональных данных.

2.9. Машинные носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

2.10. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные ему машинные носители изымаются уполномоченным сотрудником, на которого возложены функции хранения машинных носителей.

3. ПОРЯДОК УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основанием для уничтожения машинных носителей ПДн является повреждение машинного носителя, исключающее его дальнейшее использование, или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает Администратор безопасности ИСПДн. Списанные машинные носители, подлежащие уничтожению, хранятся у Администратора безопасности ИСПДн в месте, запираемом под ключ и отделенном от других машинных носителей.

Уничтожение производится путем их физического разрушения с предварительным уничтожением содержащейся на них ПДн, если это позволяют физические принципы работы носителя. Уничтожение машинных носителей осуществляется Комиссией Министерства финансов КБР по уничтожению персональных данных. Составляется Акт об уничтожении материальных носителей персональных данных (Приложение №2). После уничтожения машинные носители данных снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале учета выдачи машинных носителей персональных данных Министерства финансов КБР.

4. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ С МАШИННОГО НОСИТЕЛЯ

Хранящиеся на машинных носителях и потерявшие актуальность персональные данные своевременно уничтожаются. Основанием для уничтожения записей или части записей с машинного носителя являются следующие случаи:

- возврат носителя работником;
- передача носителя в ремонт;
- списание носителя.

Администратор безопасности информационных систем персональных данных принимает окончательное решение о необходимости уничтожения персональных данных, при получении носителя должен обеспечить уничтожение записей или части записей с носителя и подготовить Акт об уничтожении персональных данных с материального носителя (Приложении 3).

5. Ответственность

5.1. Пользователи и администраторы ИС, нарушившие требования настоящей рабочей инструкции, несут ответственность за совершенные действия в соответствии с действующим законодательством.

5.2. Пользователи и администраторы ИС, осуществляющие вынос машинных носителей за пределы служебных помещений в целях выполнения своих должностных обязанностей или заданий руководителя, не противоречащих должностным обязанностям, несут персональную ответственность за их сохранность.

Приложение № 1
к Инструкции учёта, хранения машинных носителей персональных данных в Министерстве финансов КБР
от _____г. № ____

Журнал учета выдачи машинных носителей
персональных данных в Министерстве финансов КБР

№ п/п	Регистрационный номер	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования)/ дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Отметка об уничтожении машинного носителя	Дата	Примечание
1											
2											
3											
4											

Приложение № 2
к Инструкции учёта, хранения машинных носителей персональных данных в Министерстве финансов КБР
от _____ 20 г № ____

АКТ № _____
Об уничтожении машинных носителей персональных данных
от _____г.

Комиссия в составе:

Председатель Комиссии – _____
Члены Комиссии: _____ _____ _____ _____
составила настоящий Акт о том, что произведено уничтожение машинных носителей, предназначенных для обработки (хранения) персональных данных в составе:
_____
(тип носителя, учетный номер носителя)
_____
(тип носителя, учетный номер носителя)
Носители уничтожены путем сжигания/размагничивания/физического уничтожения.

Председатель Комиссии _____ /Ф.И.О./
подпись
Члены Комиссии _____ /Ф.И.О./
подпись

Приложение № 3
к Инструкции учёта, хранения машинных носителей персональных данных в Министерстве финансов КБР
от _____ 20 г № ____

А К Т № _____
Об уничтожении персональных данных с машинного носителя
от _____г.

В связи с возвратом носителя работником / передачей носителя в ремонт/списанием носителя, произведено уничтожение персональных данных со следующих материальных носителей:

_____
(тип носителя, учетный номер носителя, основание для уничтожения персональных данных)

_____
(тип носителя, учетный номер носителя, основание для уничтожения персональных данных)

Персональные данные уничтожены с материальных носителей персональных данных с применением программного обеспечения _____
(название программного обеспечения)

Администратор безопасности
информационных систем
персональных данных _____ /Ф.И.О./
подпись

Приложение № 4
к Инструкции учёта, хранения машинных носителей персональных данных в Министерстве финансов КБР
от _____ 20 г № ____

АКТ
утери машинных носителей информации

_____
должности, ФИО

N п/п	**Дата**	***Учетный номер машинного носителя***	**Примечание**

Всего машинных носителей _____(цифрами и прописью)
На машинных носителях хранилась следующая информация:
_____
_____
Носители были утеряны _____(дата) при следующих обстоятельствах:
_____
_____
_____
Подпись пользователя _____

Подпись администратора ИБ _____

___ _____ 20___ г.