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

ПРИКАЗ

«28» ноября 2019 г. г. Нальчик № 119

О мерах по обеспечению безопасности персональных данных при их обработке в Министерстве финансов Кабардино-Балкарской Республики

п р и к а з ы в а ю :

1. Утвердить меры по обеспечению безопасности персональных данных при их обработке в Министерстве финансов Кабардино-Балкарской Республики.

2. Считать утратившим силу приказ Министерства финансов КБР от 16.11.2015 г. № 146 «О мерах по обеспечению безопасности персональных данных при их обработке».

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

И.о. министра Е.А. Лисун

Утверждены приказом
Министерства финансов КБР
от « » 20 г. №

Меры по обеспечению безопасности персональных данных при их обработке в Министерстве финансов Кабардино-Балкарской Республики

1.Общие положения

Меры по обеспечению безопасности персональных данных при их обработке в Министерстве финансов КБР разработаны с учетом Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Состав и содержание мер по обеспечению безопасности персональных данных

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;

- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Содержание мер по обеспечению безопасности персональных данных:

- меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности);
- меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил;
- меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения;
- меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных;

- меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;
- меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;
- меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия;
- меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных;
- меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных;
- меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы;
- меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту

персональных данных, представленных в виде информативных электрических сигналов и физических полей;

- меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных;
- меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов;
- меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

3.Реализация мер по обеспечению безопасности персональных данных

Для реализации указанных мер по обеспечению безопасности могут применяться межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации.

Для защиты персональных данных, представленных в виде информативных электрических сигналов и физических полей могут применяться следующие методы и способы защиты информации:

- использование технических средств, в защищенном исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств, в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств, с

помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

• обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

Возможные методы и способы защиты персональных данных, представленных в виде акустической (речевой) информации, заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.

4. Основные принципы определения актуальных угроз безопасности персональных данных

Выбор и реализация мер по обеспечению безопасности персональных данных в информационных системах осуществляются на основе угроз безопасности персональных данных, обрабатываемых Министерством финансов КБР, выявленных в Модели угроз безопасности ПДн (далее - Модель угроз), а также в зависимости от уровня защищенности ПДн, определенного в соответствии с постановлением Правительства от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Модель угроз разрабатывается на основе следующих методических документов:

• базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденная 15 февраля 2008 г. заместителем директора ФСТЭК России;

• методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденная 14 февраля 2008 г. заместителем директора ФСТЭК России.

5. Определение уровня защищенности ПДн

При обработке персональных данных в информационных системах устанавливаются уровни защищенности ПДн, обрабатываемых в ИСПДн, в соответствии с постановлением Правительства от 01.11.2012 г. № 1119 «Об

утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

При этом учитываются следующие исходные характеристики ИСПДн:

• категория обрабатываемых в информационной системе персональных данных;

• объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);

• заданные Министерством финансов КБР параметры безопасности персональных данных, обрабатываемых в информационной системе;

• тип угроз безопасности ПДн, актуальных для информационной системы;

• категория субъектов ПДн, чьи данные обрабатываются Министерством финансов КБР. Это могут быть сотрудники Министерства финансов КБР или иные субъекты ПДн, не являющиеся сотрудниками.

По результатам анализа исходных данных ИСПДн Министерства финансов КБР присваивается соответствующий уровень защищенности ПДн и составляется «Акт определения уровня защищенности ПДн, при их обработке в ИСПДн», утверждаемый приказом Министерства финансов КБР.

Уровень защищенности персональных данных может быть пересмотрен:

• по решению ответственного за обеспечение безопасности информационных систем персональных данных Министерства финансов Кабардино-Балкарской Республики, на основании проведенного им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной ИСПДн;

• по результатам мероприятий по контролю за выполнением Требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Для обеспечения безопасности персональных данных, обрабатываемых Министерством финансов КБР, должны быть выполнены работы, в соответствии с утвержденным планом по защите персональных данных в Министерстве финансов Кабардино-Балкарской Республики.

Все пользователи ИСПДн должны иметь доступ к ресурсам ИСПДн только в соответствии с разрешениями.

Доступ нового пользователя к ресурсам ИСПДн осуществляется следующим образом:

• ознакомление пользователя ИСПДн с приказом об организации обработки персональных данных в Министерстве финансов КБР и подписание

пользователем обязательства о неразглашении персональных данных субъектов персональных данных;

• создание в ИСПДн учетной записи пользователя и организация его доступа к объектам ИСПДн в соответствии с разрешениями.

При необходимости блокирования доступа пользователя ИСПДн к ресурсам ИСПДн (например, в случае увольнения сотрудника Министерства финансов КБР) необходимо удалить учетную запись пользователя и откорректировать список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн необходим для выполнения служебных (трудовых) обязанностей.

6. Пользователи ИСПДн

В Министерстве финансов КБР обработку ПДн и обслуживание объектов ИСПДн осуществляют:

• ответственный за обеспечение безопасности информационных систем персональных данных Министерства финансов Кабардино-Балкарской Республики;

• пользователь ИСПДн.

7. Требования к работникам Министерства финансов КБР по обеспечению безопасности персональных данных

Все сотрудники Министерства финансов КБР, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника происходит ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудники Министерства финансов КБР:

• должны быть ознакомлены с приказом об организации обработки персональных данных в Министерстве финансов КБР, обрабатываемых в Министерстве финансов КБР;

• использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним и возможность их утери или использования третьими лицами. Сотрудники Министерства финансов КБР

несут персональную ответственность за сохранность идентификаторов;

• должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации);

• должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты;

• не должны устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию;

• не должны разглашать защищаемую информацию третьим лицам, которая стала им известна при работе в ИСПДн Министерства финансов КБР;

• при работе с ПДн в ИСПДн обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов;

• при завершении работы в ИСПДн обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты;

• должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн;

• обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству Министерства финансов КБР и администратору безопасности информационных систем персональных данных.