КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ ФИНАНСХЭМКІЭ И МИНИСТЕРСТВЭ
КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ ФИНАНСЛА МИНИСТЕРСТВОСУ

МИНИСТЕРСТВО ФИНАНСОВ
КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ
(МИНФИН КБР)

ПРИКАЗ

« 12 » июля 2017 г. г. Нальчик № 61

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

П р и к а з ы в а ю:

1.Внести изменения в приказ Министерства финансов КБР от 17.03.2016г. №29 «О мерах по обеспечению информационной безопасности в Министерстве финансов КБР», дополнив пунктом 6 следующего содержания: «6.Утвердить Инструкцию Министерства финансов Кабардино-Балкарской Республики по обеспечению безопасности автоматизированного рабочего места, на котором установлены средства защиты информации и обрабатываются персональные данные».

2.Утвердить Инструкцию Министерства финансов Кабардино-Балкарской Республики по обеспечению безопасности автоматизированного рабочего места, на котором установлены средства защиты информации и обрабатываются персональные данные, согласно приложения к настоящему приказу.

3. Контроль за исполнением настоящего Приказа оставляю за собой.

Министр З.А.Лихов

Приложение к приказу
Министерства финансов КБР
от « 12 » июля 2017 г. № 61

Инструкция Министерства финансов Кабардино-Балкарской Республики по обеспечению безопасности автоматизированного рабочего места, на котором установлены средства защиты информации и обрабатываются персональные данные

Инструкция Министерства финансов КБР содержит перечень требований по обеспечению информационной безопасности автоматизированного рабочего места (АРМ), на котором установлены средства защиты информации (СЗИ) и на которых обрабатываются персональные данные, описание порядка обращения с сертифицированными средствами криптографической защиты информации (СКЗИ), рекомендации по размещению, использованию и хранению технических средств.

Список сокращений

АРМ - автоматизированное рабочее место
СКЗИ - сертифицированные средства криптографической защиты
НСД - несанкционированный доступ
СЗИ - средства защиты информации
ЛВС – локальная вычислительная сеть
ПО – программное обеспечение
ОС – операционная система
HDD - жесткий диск
ПЭВМ - персональная электронно-вычислительная машина

1.Общие положения

1.1. Защита информации от несанкционированного доступа должна обеспечиваться на всех технологических этапах обработки информации, в том числе при проведении ремонтных и регламентных работ. Защита

информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором информационной безопасности.

1.2. Защита программного обеспечения и аппаратного обеспечения от НСД автоматизированного рабочего места, на котором установлены средства защиты информации и обрабатываются персональные данные, является составной частью общей задачи обеспечения безопасности в Министерстве финансов КБР. Применение средств защиты информации от НСД предполагает выполнение целого ряда мер, включающих в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил, для лиц допущенных к работе с персональными данными и конфиденциальной информаций.

Состав СЗИ, применяемых на АРМ Министерства финансов КБР зависит от способа взаимодействия АРМ с другими системами: посредством прямого подключения к сети Интернет; подключения к сети Интернет через ЛВС; подключения по выделенным каналам связи через ЛВС.

2. Использование средств защиты информации

Средства защиты информации – это специальные технические средства, используемые в Министерстве финансов КБР для предупреждения несанкционированного использования всех видов информации. Разнообразие видов используемой информации, целей защиты, вариантов угроз, применяемых технологий защиты определяют широкую номенклатуру таких средств. В каждом случае необходимости защиты информации выбирается свой конкретный тип средства.

В Министерстве финансов КБР могут инструктироваться средства защиты информации:

- коллективные, применяемые для защиты информации, используемой одновременно несколькими (многими) сотрудниками;
- индивидуальные, применяемые только одним сотрудником для защиты информации, используемой им самим;
- сетевые, применяемые для защиты в вычислительных сетях и

сетях связи.

Необходимость применения средств защиты информации определяется при информационном обследовании, при принятии решения о применении информационной техники и в других случаях.

3. Требования по размещению технических средств защиты

3.1. При размещении технических средств с установленным АРМ пользователя:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным АРМ пользователя, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3.2. К установке общесистемного и специального ПО допускаются лица, изучившие документацию на установку ПО. При установке ПО на АРМ пользователя необходимо соблюдать следующие требования:

1) на технических средствах, предназначенных для работы с АРМ пользователя, использовать только лицензионное ПО фирм-изготовителей;

2) установку ПО АРМ пользователя необходимо производить только с зарегистрированного, защищенного от записи носителя;

3) на АРМ пользователя не должны устанавливаться средства разработки ПО и отладчики;

4) должны быть предусмотрены меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлено ПО АРМ пользователя (например, путем опечатывания системного блока и разъемов АРМ пользователя);

5) после завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО на АРМ пользователя;

6) ПО устанавливаемое на АРМ пользователя, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;

- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

3.3. Средства межсетевого экранирования

Взаимодействие АРМ с объектами ЛВС организации и ресурсами сети Интернет должно быть защищено с помощью сетевого или персонального средства межсетевого экранирования.

3.4. Средства обнаружения вторжений

Взаимодействие АРМ с объектами ЛВС организации и ресурсами сети Интернет должно быть защищено с помощью сетевого или персонального средства обнаружения вторжений.

4. Порядок хранения и обращения с сертифицированными средствами криптографической защиты информации установленных на АРМ

Установка, настройка и сопровождение СКЗИ в Министерстве финансов КБР осуществляется администратором информационной безопасности Министерства финансов КБР, в соответствии с требованиями законодательства Российской Федерации и эксплуатационной документации к СКЗИ:

4.1.Запрещается полное или частичное воспроизведение, тиражирование и распространение оптических носителей, содержащих дистрибутивы СКЗИ, а также лицензионных ключей СКЗИ.

4.2.Запрещается использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

4.3.Не допускается передача АРМ Министерства финансов КБР, в которых установлены средства защиты и на которых обрабатывается информация, содержащая персональные данные и конфиденциальную информацию в организации, не имеющие лицензии на проведение работ с

установленными средствами защиты и шифровальной техникой.

4.4.Порядок хранения и использования носителей ключевой информации с ключами электронной подписи должен исключать возможность несанкционированного доступа к ним.

4.5.Сертифицированные средства криптографической защиты информации Министерства финансов КБР, ключевые носители или аппаратные средства, к которым подключаются или в которые устанавливаются СКЗИ, эталонные CD-диски (диски, инсталлирующие программные СКЗИ), должны храниться в месте, исключающем возможность НСД к ним (сейф, шкаф индивидуального пользования с замком и т.п.).

4.6.Пользователи СКЗИ, имеющие доступ к носителям ключевой информации, несут персональную ответственность за безопасность ключевой информации на них и обязаны обеспечивать её сохранность, неразглашение и нераспространение.

4.7.Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

5. Порядок действий в случае выявления нарушений информационной безопасности

5.1.Действия, предпринимаемые в случае выявления нарушений информационной безопасности, состоят в следующем:

- выявление факта нарушения;
- прекращение всех операций, связанных с участком, на котором произошло нарушение;
- принятие экстренных мер для прекращения несанкционированного доступа или использования информации;
- оповещение о нарушении;
- восстановление работоспособности информационной системы;
- расследование причин нарушения информационной безопасности;
- проверка состояния информационной безопасности по факту нарушения.

5.2.Выявление факта нарушения, как правило, происходит в ходе контроля состояния информационной безопасности, администратором сети Министерства финансов КБР.

5.3. После выявления нарушения сотрудник, который обнаружил его, обязан немедленно прекратить все операции по использованию по назначению информации и средств информатизации, которые выполнялись на участке, где произошло нарушение, а также, если необходимо, на смежных участках. Если выявлен несанкционированный доступ в категорированные помещения, всякий доступ в него должен быть прекращен.

Если на момент выявления нарушения несанкционированный доступ или использование средств информатизации и информации еще продолжаются, сотрудник, выявивший их, обязан немедленно принять меры к их прекращению. Конкретное содержание этих мер зависит от того, каков характер нарушения, то есть информационный объект какой категории попал под нарушение, какой ущерб может быть нанесен нарушением, какие побочные последствия повлечет принятие этих мер.

5.4.По возможности следует привлечь для принятия мер администратора сети, администратора по защите информации.

5.5.Ответственность за адекватность принимаемых мер несут в порядке привлечения сотрудник, выявивший нарушение, администратор сети и руководитель подразделения.

5.6.После того, как нарушение выявлено и блокировано, производится срочное оповещение о нем в следующем порядке:

– сотрудник оповещает, администратора по защите информации и администратора сети;

– администратор сети оповещает других сотрудников своего подразделения о возникновении подобного нарушения;

5.7.По факту нарушения, администратором по защите информации проводится также проверка системы информационной безопасности на тех ее участках, где подобные нарушения возможны.

6. Инструктаж

6.1.Для сотрудников Министерства финансов КБР имеющих допуск к персональным данным по правилам обеспечения информационной безопасности и поддержания их знаний, проводятся следующие виды инструктажа:

– вводный;

– периодический;

– разовый.

Инструктаж проводит администратор по защите информации.

При вводном инструктаже сообщаются сведения:

– категория должности, занимаемой сотрудником;

– перечень средств информатизации и программных продуктов, имеющихся на его рабочем месте и смежных рабочих местах, их категории;

– перечень помещений, в которые он имеет допуск, их категории;

– перечень информации, к которой он имеет допуск, и его права доступа к ней;

– порядок обеспечения безопасности информации;

– порядок использования средств защиты информации, если они имеются;

– возможные варианты нарушений информационной безопасности на конкретном рабочем месте;

– действия при выявлении нарушений информационной безопасности.

Периодический инструктаж проводится один раз в год. В периодический инструктаж включается краткое изложение вопросов вводного инструктажа и подробное – изменений по этим вопросам, произошедшим со времени предыдущего инструктажа.

Разовый инструктаж проводится при проведении отдельных мероприятий по обеспечению информационной безопасности.

6.2.Инструктаж пользователя сети, проводимый администратором сети, включает:

– перечень программных продуктов, сетевых устройств, разделов памяти сетевых устройств и информации, к которым пользователь имеет доступ в сети, права доступа пользователя и категории этих объектов информационной системы;

– порядок доступа в сеть, в том числе содержание инструкции по применению паролей;

– порядок использования средств защиты информации в сети, если они имеются;

6.3.Инструктаж во всех случаях оформляется соответствующей записью в Журнале инструктажа по информационной безопасности, который заводится для этих целей Администратором информационной безопасности, и заверяется росписью инструктируемого сотрудника и лица, проводившего инструктаж.