Къэбэрдей-Балъкъэр Республикэм лэжьыгъэмкIэ, цIыхухэр лэжьапIэкIэ къызэгъэпэщынымкIэ, социальнэ хъумэныгъэмкIэ и министерствэ

Къабарты-Малкъар Республиканы урукуу, иш бла жалчытыу эм социальный жаны бла къоруулау министерствосу

МИНИСТЕРСТВО ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОЙ ЗАЩИТЫ КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ

(МИНТРУДСОЦЗАЩИТЫ КБР)

ПРИКАЗ № 358-11/ДСП

«9» ноября 2015 г. г. Нальчик

Об организации работы по защите информации в Министерстве труда, занятости и социальной защиты Кабардино-Балкарской Республики

В целях организации работы по защите конфиденциальной информации в Министерстве труда, занятости и социальной защиты Кабардино-Балкарской Республики и его структурных подразделениях, с учетом требований Гражданского кодекса Российской Федерации, Федеральных законов от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», от 10 января 2002 года №1-ФЗ «Об электронной цифровой подписи», Указов Президента Российской Федерации от 6 марта 1997 года №188 «Об утверждении перечня сведений конфиденциального характера», от 24 января 1998 года №61 «Об утверждении перечня сведений, отнесенных к государственной тайне», постановления Правительства Российской Федерации от 5 декабря 1991 года №35 «О перечне сведений, которые не могут составлять коммерческую тайну», специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30 августа 2002 года №282-дсп:

п р и к а з ы в а ю:

1. Утвердить:

Положение об обработке и о защите информации в автоматизированных информационных системах Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики и его структурных подразделений согласно приложению №1.

Перечень сведений конфиденциального характера Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики и его структурных подразделений согласно приложению №2.

Инструкцию по учету машинных носителей информации, содержащих электронные документы конфиденциального характера, согласно приложению №3.

- Порядок учета, хранения и обращения со съемными носителями персональных данных, а также их утилизации, согласно приложению №4.
- Инструкцию по организации антивирусной защиты информационных систем, согласно приложению №5.
- Инструкцию по организации парольной защиты информационных систем, согласно приложению №6.

– Инструкцию по обеспечению информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования, согласно приложению №7.

2. Возложить ответственность за выполнение требований по защите конфиденциальной информации в соответствии с настоящим приказом и законодательством Российской Федерации на руководителей структурных подразделений Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики, осуществляющим работу с конфиденциальной информацией.

3. Руководителям структурных подразделений Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики, осуществляющим работу с конфиденциальной информацией организовать работу с конфиденциальной информацией в Министерстве труда, занятости и социальной защиты Кабардино-Балкарской Республики в соответствии с настоящим приказом.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Министр А. Тюбеев

Приложение №1
к приказу Министерства труда,
занятости и социальной защиты
Кабардино-Балкарской Республики
от «___» _____ 2015 г. № _____

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И О ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ МИНИСТЕРСТВА ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОЙ ЗАЩИТЫ КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ И ЕГО СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ

1. Общие положения

1.1. Настоящее Положение определяет порядок наделения полномочиями по обработке конфиденциальной информации (далее - ОКИ), организационную систему обработки и защиты конфиденциальной информации (далее - ЗКИ), в том числе персональных данных в автоматизированных информационных системах (далее - АИС) Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики и его структурных подразделений (далее - министерство и подразделения).

1.2. Настоящее Положение не распространяется на вопросы защиты информации, содержащей государственную тайну.

1.3. Обработка конфиденциальной информации - действия (операции) с конфиденциальной информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание (персональных данных), блокирование, уничтожение.

1.4. Оператор обработки конфиденциальной информации - Министерство труда, занятости и социальной защиты Кабардино-Балкарской Республики и его структурные подразделения, организующие и (или) осуществляющие обработку конфиденциальной информации, а также определяющие цели и содержание обработки конфиденциальной информации.

2. Цели обработки и защиты конфиденциальной информации

2.1. Основной целью ОКИ в АИС является повышение эффективности исполнения министерством и подразделениями установленных законодательством полномочий.

2.2. Основными целями ЗКИ в АИС министерства и подразделений являются:

- предотвращение неконтролируемого распространения конфиденциальной информации в результате ее разглашения работниками или получения несанкционированного доступа к информации;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в АИС министерства и подразделений;
- предотвращение утрат, несанкционированного уничтожения или сбоев функционирования машинных носителей информации, обеспечение полноты, целостности, достоверности информации в АИС;
- соблюдение правового режима использования АИС;
- обеспечение возможности обработки и использования конфиденциальной информации работниками министерства и подразделений, имеющими соответствующие полномочия.

3. Организационная система обработки и защиты конфиденциальной информации

3.1. Операторами ОКИ в АИС министерства и подразделений являются структурные подразделения Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики, которые назначаются исполняющими функции оператора по ОКИ в порядке, устанавливаемом настоящим Положением.

3.2. Организационную систему ОКИ и ЗКИ в АИС министерства и подразделениях образуют:

1) Министр труда, занятости и социальной защиты Кабардино-Балкарской Республики - осуществляет общее руководство по вопросам ОКИ и ЗКИ в АИС министерства.

2) Заместитель министра труда, занятости и социальной защиты Кабардино-Балкарской Республики - осуществляет распорядительные функции по организации работ по ОКИ и ЗКИ в АИС.

3) Руководители структурных подразделений Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики - операторов, исполняющих функции операторов АИС, в которых производится ОКИ, - организуют работы по ОКИ и ЗКИ в АИС подразделений Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики, осуществляют непосредственное руководство реализацией мероприятий по ЗКИ в АИС подразделений Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики и несут ответственность за организацию ОКИ и ЗКИ в подразделениях Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики.

4) Сотрудники, ответственные за информационную безопасность в министерстве и подразделениях (далее - Администраторы ИБ) - обеспечивают выполнение организационных мероприятий по обеспечению ЗКИ в АИС министерства и подразделений; обеспечивают исполнение работ по технической защите информации (далее - ТЗИ) в АИС министерства и подразделений, несут ответственность за исполнение мероприятий по ЗКИ и соблюдение требований информационной безопасности пользователями подразделений.

5) Отдел автоматизации и информационных технологий информационно-аналитического департамента Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики (далее - отдел информатизации) - организует работу по технической защите информации в АИС министерства и подразделений, осуществляет ведение Реестра АИС министерства и подразделений, в которых осуществляется ОКИ (далее - Реестр АИС ОКИ, Реестр).

6) Пользователи (потребители) информации (далее - Пользователи) - работники, наделенные соответствующими правами по доступу к информации и непосредственно использующие информацию для исполнения своих должностных обязанностей или выполняющие непосредственные действия по вводу, обработке и передаче информации.

7) Технические специалисты - работники министерства и подразделений, сотрудники сторонних организаций, привлекаемые к работам в министерстве и подразделениях на основании договоров, осуществляющие технические действия по эксплуатации средств вычислительной техники и АИС министерства и подразделений.

3.3. Для проведения работ по ЗКИ в АИС министерства и подразделениях могут привлекаться на договорной основе специализированные организации, имеющие соответствующие лицензии на право проведения работ в области защиты информации.

3.4. Обязанности за соблюдение мер по обеспечению информационной безопасности конфиденциальной информации включаются в должностные обязанности работников, участвующих в ОКИ.

3.5. При наделении должностными обязанностями, предусматривающими работу с конфиденциальной информацией, работники должны быть под роспись ознакомлены с требованиями нормативных и руководящих документов в области ОКИ и ЗКИ и настоящего Положения в части, их касающейся, а также с ответственностью за нарушение требований по ОКИ и ЗКИ.

4. Документационная система обработки и защиты конфиденциальной информации

4.1. Документационную систему ОКИ и ЗКИ в министерстве и подразделениях образуют:

1) Перечень сведений конфиденциального характера министерства и подразделений.

2) Перечень защищаемых информационных систем в министерстве и подразделениях.

3) Инструкция по обращению с носителями конфиденциальной информации.

4) Перечни АИС подразделений министерства, в которых обрабатывается конфиденциальная информация.

5) Приказы министерства о разработке (приобретении), внедрении и организации эксплуатации АИС.

6) Должностные инструкции работников, ответственных за ЗКИ, отдельные положения в должностных инструкциях, определяющие полномочия по ОКИ.

7) Эксплуатационная документация на АИС, в которых осуществляется ОКИ.

8) Акты классификации АИС, в которых осуществляется ОКИ.

9) Технические паспорта на АИС, в которых осуществляется ОКИ.

10) Аттестаты соответствия требованиям по безопасности информации на объекты информатизации.

11) Перечни лиц, допущенных к ОКИ.

12) Инструкции по эксплуатации средств защиты информации.

13) Журнал (карточки) учета средств защиты информации.

14) Настоящее Положение.

5. Объекты защиты конфиденциальной информации

5.1. Объектами ЗКИ в АИС Администрации и подразделений являются: информация, ее материальные носители, программные и технические средства обработки и передачи информации (далее - Активы).

5.2. Защите подлежат следующие Активы:

1) Информационные ресурсы, содержащие сведения, отнесенные к категории конфиденциальной информации, представленные в виде отдельных документов, информационных массивов и баз данных, зафиксированных на машинных носителях.

2) Основные технические средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и программное обеспечение), телекоммуникационные системы, используемые для обработки и передачи информации, содержащей сведения, отнесенные к конфиденциальной информации.

3) Вспомогательные технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация, содержащая сведения, отнесенные к конфиденциальной информации.

6. Назначение оператора обработки конфиденциальной информации

6.1. С целью реализации установленных законодательством полномочий структурные подразделения министерства, планирующие создание АИС ОКИ, вносят в установленном порядке проект приказа об ОКИ в АИС структурного подразделения министерства, в котором определяются цель, правовые основания, содержание ОКИ, категории объектов учета (для обработки персональных данных - категории субъектов персональных данных), организационная система ОКИ (оператор, круг взаимодействующих в процессе ОКИ организаций и должностных лиц, предполагаемый круг пользователей, субъекты контроля и ЗКИ), предполагаемый класс АИС, дата начала ОКИ, срок или условие прекращения ОКИ, перечень мероприятий по ЗКИ, регламент ОКИ. С целью обеспечения регистрации АИС ОКИ в Реестре АИС ОКИ (п. 6.5) в список рассылки постановления включается отдел информатизации.

6.2. Должностное лицо, осуществляющее распорядительные функции в организационной системе обработки и защиты конфиденциальной информации (п. 3.3), распоряжением Администрации (п. 6.1) назначает оператора ОКИ, определяет других субъектов ОКИ и ЗКИ.

6.3. При создании АИС обработки персональных данных в установленных Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» случаях, руководители структурного подразделения - оператор обработки персональных данных направляют в уполномоченный орган по защите прав субъектов персональных данных уведомления об обработке персональных данных в соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных».

6.4. Сведения об АИС ОКИ регистрируются в Реестре АИС ОКИ отделом информатизации (п. 3.3) на основании распоряжения об ОКИ (п. 6.2).

7. Основные направления и методы ЗКИ

7.1. Основными направлениями работы по ЗКИ являются:

- физическая защита помещений, в которых обрабатывается конфиденциальная информация, от проникновения посторонних лиц;
- физическая защита Активов от хищения, разрушения, уничтожения;
- защита от НСД к конфиденциальной информации, от несанкционированного или непреднамеренного воздействия;
- защита от преднамеренных или непреднамеренных действий Пользователей, ведущих к утечке или утрате конфиденциальной информации.

7.2. Мероприятия по ЗКИ включают в себя организационно-распорядительные, технические и контрольно-корректирующие мероприятия.

7.3. Организационно-распорядительные мероприятия по ЗКИ включают в себя:

- разработку организационно-распорядительных документов по ЗКИ;
- ограничение числа лиц, допущенных к обработке конфиденциальной информации;
- организацию контролируемой зоны, размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ, ограничение доступа лиц, не допущенных к обработке конфиденциальной информации, внутрь контролируемой зоны;
- размещение дисплеев и других средств отображения, исключающее несанкционированный просмотр информации;
- документальное оформление перечня сведений конфиденциального характера, локальных перечней АИС ОКИ подразделений, Реестра АИС ОКИ;

- инвентаризацию, учет и надежное хранение Активов, содержащих конфиденциальную информацию или посредством которых производится обработка конфиденциальной информации;
- классификацию и категорирование АИС Администрации и подразделений исходя из требований законодательства и критичности для обеспечения управления, в необходимых случаях - аттестацию АИС Администрации и подразделений;
- выявление угроз НСД к конфиденциальной информации, разработка мероприятий по нейтрализации угроз;
- организацию и соблюдение правил парольной защиты в АИС Администрации и подразделений;
- повышение квалификации, совершенствование знаний и навыков Пользователей в вопросах ЗКИ;
- дисциплинарную практику.

7.4. Мероприятия по технической защите информации включают в себя:

- организацию физической защиты помещений и технических средств обработки информации с использованием организационных мер и технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации;
- сегментацию локальных вычислительных сетей (далее - ЛВС) в подразделениях, применение в сегментах ЛВС, в которых обрабатывается конфиденциальная информация, технических средств защиты информации, соответствующих требуемому классу защиты;
- техническую реализацию системы парольной защиты для каждой АИС Администрации и подразделений, в которых обрабатывается конфиденциальная информация;
- использование сертифицированных средств защиты информации в АИС Администрации и подразделений при передаче информации по открытым каналам связи в соответствии с установленными законодательством требованиями;
- использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
- регистрацию действий Пользователей, технических специалистов, контроль несанкционированного доступа и действий Пользователей, технических специалистов и посторонних лиц;
- мероприятия по антивирусной защите в АИС Администрации и подразделений;
- реализацию системы резервного копирования информации.

7.5. Контрольно-корректирующие мероприятия по ЗКИ включают в себя:

- контроль исполнения законодательства в области ЗКИ;
- контроль исполнения организационно-распорядительных документов;
- контроль выполнения мероприятий по ТЗИ, оценка эффективности выполнения мероприятий по ТЗИ;
- выработку корректирующих воздействий, реализуемых путем издания и последующего исполнения организационно-распорядительных документов;
- применение дисциплинарных мер.

7.6. Объем принимаемых мер по ЗКИ, в зависимости от возможного ущерба в случае ее утечки, разрушения или утраты определяют министр и руководители ее структурных подразделений.

8. Обязанности работников Администрации и подразделений по обработке и защите информации конфиденциального характера

8.1. Министр:

определяет организационную систему обработки и защиты конфиденциальной информации;

- осуществляет общее руководство разработкой и исполнением мероприятий по ОКИ и ЗКИ;
- взаимодействует с надзорными органами по общим вопросам обработки и защиты конфиденциальной информации в Администрации.

8.2. Заместители министр, руководители се структурных подразделений:

- осуществляют распорядительные функции по вопросам ОКИ и ЗКИ в подведомственных (руководимых) подразделениях;
- в целях реализации установленных полномочий определяют необходимость в обработке конфиденциальной информации, необходимость в ее автоматизированной обработке, вносят в установленном порядке проект постановления об ОКИ (п. 6.1), организуют разработку (приобретение) и последующую эксплуатацию АИС, определяют в соответствии с категорией обрабатываемой информации и характером обработки класс АИС;
- взаимодействуют с надзорными органами по вопросам ОКИ в АИС Администрации и подразделений;
- направляют уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных;
- принимают меры к обеспечению ЗКИ в АИС Администрации и подразделений в соответствии с действующим законодательством;
- организуют работы по подготовке к аттестации АИС Администрации и подразделений на соответствие предъявляемым требованиям;
- организуют ведение локальных перечней АИС Администрации и подразделений, в которых осуществляется ОКИ, вносят предложения по включению в Реестр АИС ОКИ, изменению или исключению соответствующих сведений в Реестре АИС ОКИ;
- утверждают списки работников, допускаемых к защищаемой информации в эксплуатируемых АИС Администрации;
- назначают Администраторов ИБ;
- принимают решения о приостановлении ОКИ в случае выявления нарушений требований по ЗКИ;
- принимают меры по фактам нарушений требований по ЗКИ, разглашения конфиденциальной информации или утери документов, содержащих такую информацию;
- определяют порядок передачи информации конфиденциального характера другим подразделениям и сторонним организациям в соответствии с установленными требованиями;
- организуют разработку и утверждают должностные инструкции, инструкции пользователей (на основе обязанностей пользователей при обработке конфиденциальной информации в автоматизированных информационных системах министерства, приложение к данному Положению), другую документацию, регламентирующую ОКИ в подведомственных (руководимых) подразделениях;
- несут персональную ответственность за состояние ЗКИ в подведомственных (руководимых) подразделениях.

8.3. Администраторы ИБ:

- разрабатывают локальные перечни АИС, эксплуатируемых в подразделении, и обеспечивают их актуализацию, готовят предложения по включению в Реестр АИС

ОКИ, изменению или исключению соответствующих сведений в Реестре АИС ОКИ;

- разрабатывают частные модели угроз для каждой из эксплуатируемых в подразделении АИС, в котором производится ОКИ, а также предложения по нейтрализации этих угроз;
- разрабатывают предложения по формированию и реализации планов мероприятий по ЗКИ;

вносят предложения об организационных мерах по ЗКИ;

- реализуют мероприятия по ТЗИ (за исключением Администраторов ИБ подразделений, не наделенных статусом юридического лица);
- ведут учет должностных лиц, допущенных к обработке конфиденциальной информации в АИС;
- организуют доведение до пользователей руководящих и методических документов по обеспечению безопасности информации с использованием сертифицированных средств криптозащиты;
- ведут учет сертифицированных средств криптозащиты, эксплуатируемых в органе Администрации района;
- ведут учет машинных носителей, предназначенных для хранения конфиденциальной информации;
- инструктируют Пользователей по вопросам ЗКИ;
- вносят предложения по повышению квалификации и обучению Администраторов ИБ, Пользователей по вопросам ЗКИ;
- контролируют уничтожение конфиденциальной информации с жестких дисков персональных компьютеров (далее - ПК) и серверов, передаваемых в ремонт или в другие подразделения;
- контролируют выполнение Пользователями общих правил работы на ПК и в ЛВС, при передаче информации по каналам связи, использования сертифицированных средств криптозащиты, за организацией доступа в Интернет, соблюдение Пользователями условий хранения ключевых документов, эксплуатационной и технической документации на сертифицированные средства криптозащиты;
- контролируют характер исходящей информации, направляемой Пользователями по электронной почте другим адресатам и принимают оперативные меры к соблюдению установленных требований по ЗКИ.

8.4. Отдел информатизации:

- организует работу по ТЗИ в АИС Администрации и подразделений;
- осуществляет разработку проектов планов мероприятий по организации системы защиты информации в АИС Администрации и подразделений, участвует в исполнении планов мероприятий, представляет отчеты о состоянии системы защиты информации в АИС Администрации и подразделений;
- разрабатывает проекты распорядительных документов по вопросам ЗКИ и ТЗИ;
- вносит предложения главе Администрации, заместителям главы Администрации и руководителям ее структурных подразделений, наделенных статусом юридического лица, о приостановлении ОКИ в подведомственном (руководимом) подразделении в случае выявления существенных нарушений требований по ЗКИ;
- осуществляет ведение Реестра АИС ОКИ, включающее в себя регистрацию АИС в Реестре, внесение изменений при изменении каких-либо атрибутов АИС, предоставление Реестра в пользование в соответствии с регламентом и исключение АИС из Реестра при прекращении ОКИ в АИС, разрабатывает регламент ведения Реестра, осуществляет взаимодействие с заместителями главы Администрации района, руководителями органов Администрации района, наделенных статусом

юридического лица, по вопросам включения в Реестр сведений об АИС, их изменения или исключения сведений об АИС из Реестра;

- разрабатывает предложения по совершенствованию системы защиты информации в Администрации и подразделениях.

8.5. Пользователи:

- участвуют в ОКИ, осуществляют непосредственные действия по регистрации информации в АИС, ее обработке, передаче по сетям передачи данных, применению сертифицированных средств криптозащиты;
- используют информацию, документы, полученные из АИС в своей работе с целью реализации возложенных на них функций;
- применяют в необходимых случаях сертифицированные средства криптозащиты.

9. Ответственность за разглашение конфиденциальной информации

9.1. За разглашение информации конфиденциального характера, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение или неисполнение требований режима защиты, обработки и порядка использования этой информации работник может быть привлечен к дисциплинарной или иной ответственности, предусмотренной действующим законодательством.

Приложение
к Положению об обработке и о защите
конфиденциальной информации в
автоматизированных информационных системах
Министерства труда, занятости и социальной защиты
Кабардино-Балкарской Республики
и его структурных подразделений

ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ МИНИСТЕРСТВА ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОЙ ЗАЩИТЫ КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ И ЕГО СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ

1. При обработке конфиденциальной информации в автоматизированных информационных системах (далее - АИС) Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики и его структурных подразделениях пользователи обязаны:

- знать и соблюдать ограничения, связанные с обработкой конфиденциальной информации (далее - ОКИ);
- знать и соблюдать правила работы с персональными компьютерами (далее - ПК) и другими средствами вычислительной техники, правила работы в локально-вычислительных сетях;
- знать и соблюдать меры по защите конфиденциальной информации (далее - ЗКИ) в АИС;
- знать и исполнять требования эксплуатационной документации на АИС;
- при работе с АИС выполнять только служебные задания;
- при работе с машинными носителями использовать только учтенные в установленном порядке машинные носители (дискеты, флэш-карты и т.п.);
- перед началом работы на ПК проверить свои рабочие папки на жестком магнитном диске, рабочие съемные машинные носители информации на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности ПК. При необходимости использования съемных машинных носителей, поступивших из сторонних организаций, прежде всего, провести проверку этих носителей на отсутствие вирусов. При сообщениях тестовых программ о появлении вирусов немедленно прекратить работу, доложить администратору информационной безопасности (далее - Администратору ИБ) и своему непосредственному руководителю;
- выполнять предписания Администратора ИБ;
- представлять для контроля свой ПК Администратору ИБ, специалисту отдела информатизации Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики при осуществлении ими действий по контролю за выполнением правил по ЗКИ;
- сохранять в тайне свой индивидуальный пароль, периодически изменять его и не сообщать другим лицам. Вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;
- располагать дисплей таким образом, чтобы исключить несанкционированное ознакомление лиц, не допущенных к обработке конфиденциальной информации, с отображаемыми сведениями;

- учет, размножение, обращение печатных материалов, содержащих сведения конфиденциального характера и имеющих гриф «Для служебного пользования», проводить в соответствии с требованиями Положения о порядке обращения со служебной информацией ограниченного распространения;
- при обнаружении различных неисправностей в работе компьютерной техники или локально-вычислительной сети, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить непосредственному руководителю и Администратору ИБ.

2. Пользователю при работе запрещается:

- предоставлять свой ПК в пользование другим работникам, посторонним лицам, кроме случаев, связанных с техническим обслуживанием техническими специалистами, осуществляющими эксплуатацию средств информатизации, или осуществлением контрольных функций Администратором ИБ или специалистами отдела информатизации;
- передавать другим лицам персональные пароли;
- самостоятельно устанавливать компьютерные программы на свой ПК;
- перенастраивать программное обеспечение ПК;
- самостоятельно вскрывать ПК и другие средства вычислительной техники;
- запускать на своем ПК любые системные или прикладные программы, кроме установленных техническими специалистами, осуществляющими эксплуатацию средств информатизации;
- изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла;
- оставлять включенным без присмотра свой ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было в доступном для других лиц месте свое персональное устройство идентификации (при наличии), машинные носители и распечатки, содержащие конфиденциальную информацию;
- производить копирование защищаемой информации на неучтенные носители;
- отсылать по электронной почте информацию, не связанную с исполнением служебных обязанностей, а также информацию по просьбе третьих лиц без согласования с руководителем структурного подразделения;
- запрашивать и получать из сети Интернет материалы развлекательного характера (игры, клипы и т.д.), кроме случаев их использования в служебных целях (только по согласованию с руководителем структурного подразделения;
- запрашивать и получать из сети Интернет программные продукты, базы данных, обновления программных продуктов и баз данных, кроме случаев, связанных с исполнением служебных обязанностей;
- входить в другие компьютерные системы через локально-вычислительную сеть министерства без разрешения операторов этих систем и предоставления допуска в установленном порядке;
- использовать в личных целях сведения конфиденциального характера, ставшие известными вследствие выполнения служебных обязанностей.

Приложение №2
к приказу Министерства труда,
занятости и социальной защиты
Кабардино-Балкарской Республики
от «___» _____ 2015 г. №_____

ПЕРЕЧЕНЬ
СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА
МИНИСТЕРСТВА ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОЙ ЗАЩИТЫ
КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ И ЕГО СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ

1. Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (персональные данные).

2. Сведения о планируемых изменениях в структуре министерства и его структурных подразделениях.

3. Штатное расписание работников.

4. Сведения о местах и условиях хранения материальных ценностей.

5. Сведения об остатках на счетах министерства и его подведомственных учреждениях.

6. Сведения о путях и способах получения информации из бухгалтерской автоматизированной базы данных.

7. Сводные сведения о поступлении денежных средств на расчетные счета министерства.

8. Сводные сведения о списании денежных средств с расчетных счетов министерства и его подведомственных учреждениях.

9. Сводные сведения о результатах анализа финансово-хозяйственной деятельности за месяц, квартал, год.

10. Сводные сведения о действующей системе по оплате и мотивации труда, льготах, компенсациях, медицинском обслуживании, страховании работников.

11. Содержание данных налогового учета (в том числе данных первичных документов) является налоговой тайной.

12. Выводы до завершения ревизии (проверки) и оформления ее результатов в виде акта (заключения).

13. Сведения, представляемые гражданами при обращении в министерство и его подведомственные учреждения.

14. Структура построения локальной вычислительной сети (ЛВС) министерства и его подведомственных учреждениях.

15. Значения кодов и паролей для ПК от несанкционированного доступа.

16. Сведения о создании и функционировании АИС министерства и его подведомственных учреждениях.

17. Сведения о методах и способах обеспечения информационной безопасности в ЛВС министерства и его подведомственных учреждениях.

18. Информация и документы, в которых рассматриваются вопросы защиты информации, создаваемой, обрабатываемой и хранящейся в средствах вычислительной техники, а также циркулирующей в ЛВС министерства и его подведомственных учреждений.

19. Сведения о методах, средствах, эффективности защиты информации от разрушения, искажения, утечки или несанкционированного доступа в процессе ее создания, обработки, хранения или распространения в АИС, средствах вычислительной техники, других технических средствах.

20. Сведения в области геодезии, топографии, картографии, аэросъемок.

21. Сведения о мобилизационной подготовке не отнесенные к государственной тайне.

22. Сведения по учету и бронированию военнообязанных по отдельным организациям, в которых работает менее 300 человек военнообязанных.

23. Информация о переподготовке и повышении квалификации специалистов в области мобилизационной подготовки.

24. Сведения о наличии в организациях защитных сооружений гражданской обороны (далее - ГО), средств индивидуальной защиты ГО, специальных формирований ГО, переписка и принимаемые решения по этим вопросам.

25. Совокупные сведения о мероприятиях, направленных на предотвращение чрезвычайных ситуаций.

26. Сведения по испытанию защитных или специальных сооружений ГО на соответствие санитарно-гигиеническим и санитарно-техническим нормам.

27. Сведения о фактическом состоянии технических средств охраны, схемных и конструкторских решениях, применяемых в охранных, противопожарных системах сигнализации, данные об организациях - изготовителях используемой охранной техники, организациях, осуществляющих ее монтаж и ведущих обслуживание, ответственных за режим лицах, планах усовершенствования систем охраны и имеющихся недостатках (если сведения не отнесены к категории секретных).

28. Материалы служебных расследований.

29. Сведения об организации контрольных мероприятий и проверок.

30. Государственная статистическая отчетность.

Приложение №3
к приказу Министерства труда,
занятости и социальной защиты
Кабардино-Балкарской Республики
от «___» _____ 2015 г. №_____

ИНСТРУКЦИЯ
ПО УЧЕТУ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, СОДЕРЖАЩИХ ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

1. Конфиденциальная информация, содержащаяся в документах, имеющих обращение к Министерству труда, занятости и социальной защиты Кабардино-Балкарской Республики и его структурные подразделения, является служебной информацией ограниченного распространения.

2. На съемных машинных носителях информации (дискетах, магнитооптических дисках и т.д.), содержащих электронные документы конфиденциального характера, проставляется пометка «Для служебного пользования» (ДСП).

3. Учет (регистрация) отпечатанных с помощью средств вычислительной техники документов, содержащих информацию конфиденциального характера, осуществляется в порядке, определенном для бумажных носителей информации. Машинные носители информации с конфиденциальной информацией учитываются по журналу учета машинных носителей информации. Учетные реквизиты (учетный номер, дата регистрации, пометка «ДСП» и т.д.) проставляются на машинных носителях информации в удобном для просмотра месте.

Машинные носители информации с пометкой «ДСП»:

- регистрируются в структурном подразделении министерства, которому поручен учет документов с пометкой «ДСП», с проставлением учетных реквизитов;
- передаются другим исполнителям под расписку в журнале учета машинных носителей информации или по карточке учета;
- уничтожаются по акту.

3. Порядок рассылки, уничтожения, передачи, проверки наличия машинных носителей информации, проведения расследований по фактам утраты машинных носителей информации, снятия пометки «Для служебного пользования» с машинных носителей информации и т.д. является таким же, как и для документов конфиденциального характера.

Приложение №4
к приказу Министерства труда,
занятости и социальной защиты
Кабардино-Балкарской Республики
от «_ » _ _ _ 2015 г. № _ _ _

ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ ИХ УТИЛИЗАЦИИ

1. Все находящиеся на хранении и в обращении съемные носители с персональными данными и конфиденциальной информации подлежат учету. Такой съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

2. Учет и выдачу съемных носителей с записью в журналах учета машинных носителей информации осуществляют руководители соответствующих структурных подразделений министерства, а в территориальных структурных подразделениях по опеке и попечительству - ответственные за ведение делопроизводства для служебного пользования.

3. Не допускается хранение съемных носителей с персональными данными и конфиденциальной информацией вместе с носителями открытой информации, на рабочих столах либо оставление их без присмотра или передача на хранение другим лицам.

4. О фактах утраты съемных носителей, содержащих персональными данными и конфиденциальную информацию, либо разглашения содержащихся на них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения министерства. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей информации.

5. Съемные носители персональных данных и конфиденциальной информации, приведшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей осуществляется соответствующей комиссией, состав которой утверждается приказом министерства. Результаты уничтожения носителей оформляются актом.

Приложение №5
к приказу Министерства труда,
занятости и социальной защиты
Кабардино-Балкарской Республики
от «__» _____ 2015 г. № _____

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в Министерстве труда, занятости и социальной защиты Кабардино-Балкарской Республики (далее - министерство), с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы и возникновения фактов заражения программного обеспечения (далее - программного обеспечения) компьютерными вирусами.

1.2. В настоящей Инструкции использованы следующие термины и определения:

1) Антивирусное программное обеспечение - набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для профилактики, предотвращения заражения файлов или операционной системы вредоносным кодом;

2) Антивирусные базы - файлы, используемые антивирусным программным обеспечением при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного программного обеспечения;

3) Антивирусный контроль - проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ;

4) Вредоносная программа - компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационные ресурсы;

5) Защищаемый компьютер - электронно-вычислительная машина (персональный компьютер или сервер), используемая для обработки данных;

6) Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

7) Пользователь - служащий Агентства или другое лицо, использующее в работе средства электронно-вычислительной техники Агентства;

8) Съемный носитель информации - носитель информации, предназначенный для ее автономного хранения, независимо от места использования (съемные винчестеры, флеш-память, CD, DVD, дискеты и др.).

1.3. Требования настоящей Инструкции обязательны для выполнения всеми пользователями.

1.4. Общее и методическое руководство обеспечением антивирусной защиты информационной системы персональных данных в Агентстве осуществляется отделом информационных технологий и эксплуатации автоматизированных систем.

1.5. Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему объекта вычислительной техники при обработке персональных данных и выполнения других видов работ.

1.6. Техническое обслуживание средств вычислительной техники, уборка помещения и т.п. проводятся под контролем пользователя или уполномоченного лица.

2. Установка антивирусного программного обеспечения

2.1. Установку антивирусного программного обеспечения производит администратор информационной безопасности министерства.

2.2. В министерстве может использоваться только лицензионное антивирусное программного обеспечения, сертифицированное ФСТЭК России.

2.3. Установка антивирусного программного обеспечения производится индивидуально на каждый защищаемый компьютер.

2.4. Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного программного обеспечения.

2.5. Ярлык для запуска антивирусного программного обеспечения должен быть вынесен на "Рабочий стол" операционной системы.

3. Порядок обновления антивирусных баз

3.1. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети министерства, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений (по рабочим дням).

3.2. Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети министерства, должно осуществляться с использованием маркированных съемных носителей информации, в обязательном порядке проверяемых антивирусным программным обеспечением перед их использованием или принудительным подключением к локальной сети служащими отдела информационных технологий и эксплуатации автоматизированных систем.

3.3. Проверка критических областей защищаемого компьютера, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

3.4. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети министерства, контролируется пользователем самостоятельно ежедневно и в случае нарушения пользователь должен не принимать никаких мер и срочно сообщить администратору информационной безопасности.

4. Требования к проведению антивирусного контроля

4.1. Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

4.2. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также данные на съемных носителях информации. Контроль входящей и исходящей информации на защищаемых компьютерах должен осуществляться непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения.

4.3. Все программное обеспечение, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ.

4.4. Не реже одного раза в две недели должна проводиться полная проверка всех файлов, хранящихся на жестких дисках защищаемого компьютера.

4.5. Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера должен выполняться:

- сразу после установки или изменения программного обеспечения;
- после подключения автономного компьютера к локальной сети;

- при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4.6. В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь администратора информационной безопасности.

5. Действия пользователей при обнаружении вредоносных программ

5.1. В случае обнаружения при проведении антивирусной проверки вредоносных программ пользователи обязаны:

- приостановить все операции, связанные с обработкой файлов на защищаемом компьютере;
- немедленно поставить в известность о факте обнаружения вредоносных программ непосредственного начальника отдела, владельцев зараженных или поврежденных вредоносными программами файлов, другие отделы, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение зараженных файлов совместно с администратором информационной безопасности;
- в случае обнаружения не поддающегося лечению вируса, пользователь обязан удалить инфицированный файл в соответствующую папку антивирусного ПО, и проверить работоспособность компьютера совместно с администратором информационной безопасности.

6. Ответственность за выполнение требований инструкции

6.1. Ответственность за организацию антивирусной защиты информации на компьютерах несет начальник отдела автоматизации и информационных технологий.

6.2. Ответственность за соблюдение требований настоящей Инструкции несут пользователи.

6.3. Ответственность за своевременное обновление антивирусных баз на сервере обновлений несет администратор информационной безопасности.

6.4. Ответственность за своевременное обновление антивирусных баз и получение новых лицензионных ключей при истечении их срока действия несет администратор информационной безопасности.

Приложение №6
к приказу Министерства труда,
занятости и социальной защиты
Кабардино-Балкарской Республики
от «___» _____ 2015 г. №_____

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

1. Общие положения

1.1. Настоящая Инструкция определяет порядок защиты ресурсов автоматизированных систем, обрабатывающей конфиденциальной информации, с использованием подсистемы парольной защиты от несанкционированного доступа в автоматизированных системах объекта информатизации Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики (далее - министерство), предназначенных для обработки конфиденциальной информации.

1.2. Парольная защита при работе на объекте информатизации осуществляется с целью предотвращения несанкционированного доступа к информации, содержащей сведения ограниченного доступа.

1.3. Парольная защита объекта информатизации является составной частью подсистемы управления доступом общей системы защиты от несанкционированного доступа.

1.4. К основным видам паролей относятся:

- пароли доступа к локальным ресурсам отдельного компьютера объекта информатизации;
- пароли доступа к прикладным программам, обеспечивающим доступ к информации;
- пароль доступа средств защиты от несанкционированного доступа;
- пароли систем доступа встроенных в используемые операционные системы.

2. Требования к организации парольной защиты объекта информатизации

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в защищаемых автоматизированных системах возлагается на администратора информационной безопасности.

2.2. Личные пароли доступа к ресурсам в автоматизированных системах, системе защиты от несанкционированного доступа, а также пароли встроенных в операционные системы доступа выбираются пользователями самостоятельно, но при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры и специальные символы;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования АРМ организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM и т.п.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, QWERTY, 123456 или 1йфячып2 и т.п.);
- не использовать ранее использованные пароли;
- минимальное время применения пароля - не менее 2 дней;
- максимальное время применения пароля - не более чем 90 дней.

2.3. Лица, использующие парольную защиту, обязаны:
четко знать и строго выполнять требования настоящей Инструкции;
своевременно сообщать администратору информационной безопасности обо всех нештатных ситуациях, нарушениях работы подсистем защиты от несанкционированного доступа, возникающих при работе с паролями.

2.4. При организации парольной защиты запрещается:
записывать свои пароли в очевидных местах (внутренние стенки ящика стола, на передней панели монитора, на обратной стороне клавиатуры и т.д.);
хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;
сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от несанкционированного доступа.

2.5. Начальник отдела информационных технологий и эксплуатации автоматизированных систем несет личную ответственность за организацию работы в министерстве по безусловному выполнению требований настоящей Инструкции.

2.6. Ответственность за непосредственную работу с паролями (своевременный ввод в действие, замену и уничтожение) возлагается на администратора информационной безопасности.

2.7. На администратора информационной безопасности возлагаются следующие задачи:
- обеспечение функционирования системы парольной защиты;
- контроль за реализацией требований по обеспечению безопасности при использовании паролей на объектах информатизации.

3. Порядок применения парольной защиты

3.1. Защита с применением паролей для технических средств и программных продуктов осуществляется в соответствии с эксплуатационной документацией на эти средства.

3.2. Внеплановая смена (удаление) личного пароля любого пользователя автоматизированной системы должна производиться в следующих случаях:
в случае прекращения полномочий (увольнение, перемещение по должности) лица, допущенного к обработке информации на объекте информатизации;
после обнаружения факта успешной попытки несанкционированного доступа к элементам защищаемого объекта информатизации;
при обнаружении факта компрометации базы данных, содержащей пароли пользователей.

3.3. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администратора информационной безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем автоматизированных систем.

3.4. Для предотвращения доступа к информации ограниченного доступа, находящейся на несъемных магнитных носителях, пользователь по окончании сеанса работы или во время перерыва в работе обязан осуществить выход из системы и выключить автоматизированное рабочее место (далее - АРМ).

3.5. Пароли, используемые для локального доступа к программным средствам и к ресурсам объекта информатизации, вводятся пользователем с клавиатуры.

3.6. Компрометация действующих паролей является чрезвычайным происшествием, о чем пользователь сообщает администратору информационной безопасности.

3.7. Скомпрометированные пароли выводятся из действия немедленно.

3.8. Пользователь в случае компрометации действующих паролей принимает меры по предотвращению работы с АРМ, где используются скомпрометированные пароли, до ввода новых паролей, сообщив немедленно о случившемся администратору информационной безопасности.

3.9. С получением информации о случае компрометации паролей администратор информационной безопасности проводит анализ и оценку данного случая, после чего изменяет пароли в системе защиты информации от несанкционированного доступа.

3.10. По каждому случаю, связанному с компрометацией действующих паролей, администратор информационной безопасности организует и проводит служебную проверку. По результатам расследования к лицам, допустившим разглашение паролей, применяются необходимые административные или дисциплинарные меры.

Приложение №7
к приказу Министерства труда,
занятости и социальной защиты
Кабардино-Балкарской Республики
от «___» _____ 2015 г. №_____

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДКЛЮЧЕНИИ И ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ

1. Общие положения

1.1. Инструкция по обеспечению информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики (далее - министерство) устанавливает требования к работе в сети Интернет служащих министерства.

1.2. В настоящей Инструкции используются следующие термины и определения:

- Интернет - глобальная информационная система, имеющая логически взаимосвязанное единое адресное пространство, являющаяся совокупностью общедоступных информационных сетей и основанная на использовании стека протоколов TCP/IP (протокол управления передачей/интернет-протокол);
- Администратор - лицо, ответственное за использование, техническое обеспечение и функционирование средств вычислительной техники, имеющих выход в сеть Интернет;
- Пользователь - лицо, допущенное к работе в сети Интернет;
- Логин - регистрационное имя пользователя, выраженное комбинацией цифр, букв и (или) знаков;
- Пароль - кодовая комбинация, состоящая из букв, цифр и (или) знаков, подтверждающая правомочность пользователя на осуществление входа в сеть Интернет с определенным для него логином;
- Ресурс (сайт) - логическая и (или) физическая часть вычислительной системы и совокупность информационных ресурсов, предназначенных для общего доступа пользователю, подключенному к сети Интернет, имеющему соответствующие технические средства, получить доступ к части или всей информации на платной или бесплатной основе;
- Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

1.3. Работники, использующие ресурсы сети Интернет, подразделяются на следующие категории: администратор и пользователь.

2. Требования, предъявляемые к порядку подключения и организации работы в сети интернет

2.1. Приказом министра назначается администратор информационной безопасности.

2.2. Подключение работников к сети Интернет проводится с обоснованной служебной необходимостью.

2.3. Подключение к информационным ресурсам сети Интернет технических средств, информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие служебную и иную охраняемую законом тайну, а также для которых установлены особые правила доступа, без технических средств защиты информации запрещается.

2.4. Включение технических средств, информационных систем, сетей связи и автономных персональных компьютеров, проводится при обязательном использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических, для подтверждения достоверности информации (антивирусное программное обеспечение, система защиты от несанкционированного доступа, межсетевые экраны и другие средства защиты).

2.5. Размещение технических средств, подключаемых к открытым информационным системам и сетям связи, включая сеть Интернет, используемым при информационном обмене в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения ограниченного доступа, осуществляется только при наличии сертификата запрещается.

2.6. Контроль доступа к ресурсам сети Интернет работников министерства возлагается на администратора информационной безопасности.

3. Функции администратора информационной безопасности при организации работы в сети интернет

3.1. Администратор информационной безопасности выполняет следующие функции:

3.1.1. Организует допуск пользователей к работе в сети Интернет;

3.1.2. Обеспечивает инсталляцию, настройку, обновление программного обеспечения систем защиты от несанкционированного доступа и реализацию требований информационной безопасности и автоматического учета времени работы пользователей на технических средствах, подключенных к сети Интернет;

3.1.3. Обеспечивает работоспособность и актуализацию системы антивирусной защиты рабочих мест, подключенных к сети Интернет;

3.1.4. Незамедлительно докладывает начальнику отдела информационных технологий и эксплуатации автоматизированных систем о фактах нарушения требований настоящей Инструкции и попытках несанкционированного доступа к техническим средствам, за которые он несет ответственность;

3.1.5. В случае нарушения требований настоящей Инструкции, по указанию руководства Агентства, прекращает допуск пользователей к использованию ресурсов сети Интернет.

4. Требования к использованию сети Интернет

4.1. Пользователи обязаны:

4.1.1. Соблюдать требования настоящих Правил;

4.1.2. Соблюдать при доступе к ресурсам сети Интернет правила, установленные владельцами используемых ресурсов;

4.1.3. Сообщать администратору информационной безопасности о сбоях, возникших в процессе работы в сети Интернет.

4.2. Пользователям запрещается:

4.2.1. Оставлять без присмотра рабочее место, подключенное к сети Интернет;

4.2.2. Предоставлять логин и пароль другим лицам для работы в сети Интернет;

4.2.3. Использовать доступ к сети Интернет в личных целях, не связанных с выполнением служебных обязанностей;

4.2.4. Осуществлять несанкционированный доступ к информационным ресурсам сети Интернет, а также повреждать, уничтожать или фальсифицировать ее информационные ресурсы;

4.2.5. Самостоятельно устанавливать или удалять программы на компьютерах, подключенных к сети Интернет, изменять настройки операционной системы и приложений, влияющих на работу сетевого оборудования и сетевых ресурсов;

4.2.6. Изменять техническую конфигурацию средств электронной вычислительной техники, сетевого и периферийного оборудования и подключать дополнительное оборудование;

4.2.7. Передавать в сеть Интернет информацию, содержащую информацию ограниченного доступа, и (или) иные сведения, охраняемые законодательством Российской Федерации;

4.2.8. Нарушать регламент учетной системы и системы статистики, в том числе повреждать или дезинформировать вышеуказанные системы;

4.2.9. Осуществлять рассылку информации, не имеющей отношения к служебной деятельности.

4.3. В случае выявления нарушения требований настоящей Инструкции запрещается использование сети Интернет на рабочем месте до момента устранения нарушения и причин их возникновения.

4.4. Пользователь несет личную ответственность за информационный обмен, совершаемый от его имени (с его логином и паролем) и нарушение требований Инструкции.