**КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ И АРХИВ КЪУЛЫКЪУ**
**КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ АРХИВ СЛУЖБАСЫ**
**АРХИВНАЯ СЛУЖБА КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ**

# УНАФЭ БУЙРУКЪ ПРИКАЗ

31 мая 2016 г. № 39

Налшык къ. Нальчик ш. г. Нальчик

## Об утверждении Инструкции о защите информации в автоматизированных средствах Архивной службы Кабардино-Балкарской Республики

В соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
п р и к а з ы в а ю:

1. Утвердить прилагаемую Инструкцию о защите информации в автоматизированных средствах Архивной службы Кабардино-Балкарской Республики.

2. Начальнику отдела по вопросам государственной службы, кадров, противодействия коррупции и делопроизводства (Мирзаканова Е.А.) ознакомить гражданских служащих Архивной службы Кабардино-Балкарской Республики, допущенных к сведениям конфиденциального характера, с требованиями настоящей Инструкции.

3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Гуртуева А.О.

Руководитель Ш.Х. Шогенов

Согласовано:

Заместитель руководителя А.О. Гуртуев

Начальник отдела по вопросам госслужбы, кадров, противодействия коррупции и делопроизводства Е.А. Мирзаканова

Начальник отдела правового и информационного обеспечения, контроля за исполнением архивного законодательства Х.С. Курманов

В дело № 1.1.7
31.05.2016 г.
pr._39од.doc/

УТВЕРЖДЕНА
приказом Архивной службы КБР
от 31 мая 2016 г. № 39

# ИНСТРУКЦИЯ
# о защите информации в автоматизированных средствах Архивной службы Кабардино-Балкарской Республики

## 1. Общие положения

1.1. Инструкция о защите информации в автоматизированных средствах Архивной службы Кабардино-Балкарской Республики (далее - Инструкция) разработана в соответствии с федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 21 июля 1993 г. № 5485-1 «О государственной тайне», Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденным постановлением Правительства Российской Федерации от 15 сентября 1993 г. № 912-51, государственным стандартом Российской Федерации ГОСТ Р 50922-96 «Защита информации. Основные термины и определения», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Государственной технической комиссии Российской Федерации от 30 августа 2002 г. № 282.

1.2. Инструкция определяет основные меры по защите информации, типовые обязанности пользователей и должностных лиц, входящих в систему защиты информации в компьютерных и телекоммуникационных сетях Архивной службы Кабардино-Балкарской Республики (далее – Архивной службы КБР).

1.3. Требования Инструкции являются обязательными для работников Архивной службы КБР, которые допущены к работе с информацией ограниченного доступа и сведениями, составляющими государственную тайну.

При приеме на службу работники, которые будут допущены к сведениям конфиденциального характера, должны быть под расписку ознакомлены с требованиями настоящей Инструкции, в части их касающейся, а также с ответственностью за их нарушение.

1.4. В Инструкции используются следующие термины и их определения:

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аттестация** - комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Акта соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

**Абонентский пункт информационной сети общего пользования (АП ИВС ОП)** - автоматизированная система, подключаемая к информационной сети общего пользования (Интернет) с помощью коммутационного оборудования и предназначенная для работы абонентов.

**Безопасность информации** - состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системой от внутренних или внешних угроз.

**Доступ к информации** - возможность получения информации и ее использования.

**Закладное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защита информации** - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Защищаемые помещения** - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

**Информация** - сведения (сообщения, данные), независимо от формы их представления.

**Информационные ресурсы** - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

**Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационная инфраструктура** - совокупность систем обработки и анализа информации, каналов информационного обмена и телекоммуникаций, линий связи, систем и средств защиты информации.

**Информация ограниченного доступа** - информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования.

**Конфиденциальная информация** - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

**Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**Контролируемая зона** - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств, технических и иных материальных средств.

**Локальная вычислительная сеть** - совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с

другими информационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС.

**Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

**Непреднамеренное воздействие на информацию** - воздействие ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**Несанкционированное воздействие на информацию** - воздействие на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящее к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате.

**Обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора права разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

**Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

**Объект защиты информации** - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

**Оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

**Пользователь информации** - субъект, обращающийся к информационной системе за получением необходимой ему информации и пользующийся ею.

**Разглашение** - умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с информацией.

**Система защиты информации** - комплекс организационных мер и программно-технических средств обеспечения безопасности информации в автоматизированных системах.

**Средство защиты информации** - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** - совокупность объекта технической разведки, физической среды распространения информационного сигнала и средств, которыми добывается защищаемая информация.

**Технические средства приема, обработки, хранения и передачи информации** - технические средства, непосредственно обрабатывающие информацию, к средствам относятся: электронно-вычислительная техника, режимные АТС, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

## 2. Существующие угрозы информационной системе Архивной службы КБР

2.1. В настоящей Инструкции в основном регламентируются вопросы защиты конфиденциальной информации. При работе с информацией, содержащей государственную тайну, к средствам вычислительной техники (далее - СВТ), автоматизированным системам и персоналу предъявляются дополнительные требования, изложенные в документах по защите государственной тайны.

2.2. Угрозы для информации, циркулирующей в АС Архивной службы КБР, исходят от утечки по техническим каналам, от внедренных специальных электронных устройств, от специальных программ-вирусов, от несанкционированного доступа (далее - НСД).

2.3. К основным способам НСД к информации относятся:

- непосредственное обращение к объектам доступа;
- воздействие на АС программных и технических средств, позволяющих выполнить обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД;
- внедрение заинтересованными лицами в СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС, и позволяющих осуществить НСД.

2.4. Несанкционированный доступ к информации, находящейся в АС Архивной службы КБР, может быть косвенным - без физического доступа к элементам АС и прямым - с физическим доступом.

Существуют следующие пути несанкционированного доступа к информации:

- применение подслушивающих устройств;
- дистанционное фотографирование;
- перехват электромагнитных излучений;
- хищение информации;
- считывание данных в массивах других пользователей;
- копирование носителей информации;
- маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
- использование программных ловушек;
- получение защищаемых данных с помощью серии разрешенных запросов;
- использование недостатков языков программирования и операционных систем;
- преднамеренное включение в библиотеки программ специальных блоков типа «троянских коней»;

- незаконное подключение к аппаратуре или линиям связи информационной системы;

- злоумышленный вывод из строя механизмов защиты.

## 3. Основные направления и методы защиты информации

3.1. Конфиденциальная информация АС КБР подлежит обязательной защите.

3.2. Обеспечение надежной защиты информации является одной из важнейших обязанностей операторов (пользователей) информационной системы АС КБР и должностных лиц, входящих в систему защиты информации АС КБР.

3.3. Руководители структурных подразделений Архивной службы КБР контролируют в подчиненных подразделениях выполнение работниками установленных общих требований по организации работы АС и предусмотренных мер по защите информации.

3.4. Операторы информационной системы (пользователи) соблюдают правила обработки информации в АС и отвечают за обеспечение защиты информации.

3.5. Должностные лица, отвечающие за безопасность информации и входящие в систему защиты информации в компьютерных и телекоммуникационных сетях Архивной службы КБР, контролируют в пределах своей компетенции состояние защиты информации с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки ее защищенности.

В качестве программных средств используются специальные программы, предназначенные для выполнения функций, связанных с защитой информации.

К техническим средствам защиты информации относятся различные электрические, электромеханические и электронные устройства, которые подразделяются на аппаратные средства - устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с СВТ по стандартному интерфейсу и физические средства - автономные устройства (электронно-механическое оборудование охранной сигнализации и наблюдения, запоры и решетки на окнах).

3.6. Защите подлежат все компоненты информационной структуры Архивной службы КБР: документы, сети связи, ТСПИ, персонал и т.д.

3.8. Защита информации в АС Архивной службы КБР осуществляется по следующим основным направлениям:

- от утечки по техническим каналам;
- от внедренных специальных электронных устройств;
- от специальных программ-вирусов;
- от несанкционированного доступа;
- от несанкционированного воздействия;
- от непреднамеренного воздействия;
- от разглашения.

3.9. В качестве основных мер защиты информации в Архивной службе КБР должностными лицами, входящими в систему защиты информации, должны выполняться:

а) документальное оформление перечня сведений конфиденциального характера с учетом ведомственной специфики этих сведений;

б) разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

в) ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;

г) учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;

д) резервирование технических средств, дублирование массивов и носителей информации;

е) использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;

ж) использование сертифицированных средств защиты информации;

з) размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ;

и) использование защищенных каналов связи;

к) размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

л) организация физической защиты помещений и собственно технических средств обработки информации с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации;

м) предотвращение внедрения в АС программ-вирусов, программных закладок.

### 3.1. Защита информации от утечки по техническим каналам

3.1.1. При выявлении технических каналов утечки информации технические средства обработки, хранения и передачи информации рассматриваются как система, включающая основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммуникационные устройства, системы электропитания, системы заземления.

3.1.2. Отдельные технические средства или группа технических средств, предназначенных для обработки информации, вместе с помещениями, в которых они размещаются, составляют объект ТСПИ. Под объектами ТСПИ понимаются также выделенные помещения, предназначенные для проведения конфиденциальных мероприятий.

Наряду с ТСПИ, в помещениях могут находиться вспомогательные технические средства и системы (далее - ВТСС), не применяемые в обработке информации, но используемые совместно с ТСПИ и находящиеся в зоне электромагнитного поля, создаваемого ими. К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и т.д.

3.1.3. В качестве канала утечки информации основное внимание необходимо уделять ВТСС, имеющим выход за пределы контролируемой зоны.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками.

3.1.4. Основные способы защиты информации от утечки по техническим каналам:

- использование сертифицированных по требованиям защиты информации основных технических средств и систем, предназначенных для передачи, обработки и хранения конфиденциальной информации (далее - ОТСС) и ВТСС;

использование сертифицированных технических средств защиты информации;

- размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ;

- защита цепей электропитания объектов защиты;

- документальное оформление перечня защищаемых помещений (далее - ЗП) и лиц, ответственных за их эксплуатацию;

- выполнение рекомендованных мероприятий по оборудованию ЗП: стены, полы и потолки не должны быть смежными с помещениями других организаций; окна закрываются шторами (жалюзи); проведение специальных проверок помещений; применение технических средств защиты информации и т.д.);

- выполнение пожарной и охранной сигнализации только по проводной схеме сбора информации;

- применение при необходимости активных средств защиты речевого сигнала (генераторы шума и т.п.);

- выполнение требований по монтажу и применению ВТСС в ЗП согласно Специальным требованиям и рекомендациям по технической защите конфиденциальной информации;

- проведение на объектах защиты специальных исследований специализированными организациями, имеющими лицензии на проведение работ по защите информации.

### 3.2. Защита информации от внедренных специальных электронных устройств

3.2.1. Информация, обрабатываемая в ТСПИ, может сниматься путем установки в них электронных устройств перехвата информации - закладных устройств (мини-передатчики, излучение которых модулируется информационным сигналом).

3.2.2. Выявление внедренных на объекты электронных устройств перехвата информации достигается специальными проверками, которые проводятся при аттестации помещений, предназначенных для ведения секретных и конфиденциальных переговоров, а также по решению руководителя - периодически. Для помещений, предназначенных для ведения секретных переговоров, аттестация является обязательной, а для ведения конфиденциальных переговоров - добровольной.

3.2.3. Специальные проверки проводятся также с целью выявления и изъятия специальных электронных устройств перехвата информации, внедренных в ОТСС и ВТСС. Специальные проверки должны проводить специалисты организаций, имеющих лицензии, выданные уполномоченными органами.

В зависимости от целей, задач и используемых средств устанавливаются следующие виды специальных проверок:

- специальное обследование объектов защиты;
- визуальный осмотр ЗП;
- комплексная специальная проверка ЗП;
- визуальный осмотр и специальная проверка новых предметов (подарков, предметов интерьера, бытовых приборов и т.п.) и мебели, размещаемых или устанавливаемых в ЗП;
- специальная проверка применяемой радиоэлектронной аппаратуры;
- периодический радиоконтроль (радиомониторинг) ЗП;
- постоянный (непрерывный) радиоконтроль ЗП;
- специальная проверка проводных линий;
- проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов АТС.

Периодичность и виды проверок помещений в целях выявления в них закладных устройств зависят от степени важности помещений и порядка допуска в них посторонних лиц.

3.2.4. Специальное обследование и визуальный осмотр ЗП проводятся, как правило, без применения технических средств. Остальные же виды проверок требуют использования тех или иных специальных средств контроля.

3.2.5. Тестовый «прозвон» телефонных аппаратов проводится при установке нового телефонного аппарата или телефонного аппарата после ремонта, а также периодически. «Прозвон» необходимо проводить с радиотелефона или телефонного аппарата, установленного в другом помещении. При наборе номера проверяемого телефонного аппарата осуществляется контроль (на слух) прохождения всех вызывных сигналов АТС. Если обнаружено подавление (непрохождение) одного - двух вызывных звонков у контролируемого телефонного аппарата, то, возможно, что в его корпусе или телефонной линии установлено закладное устройство, и необходимо проводить специальную проверку телефонной линии и телефонного аппарата.

### 3.3. Защита информации от специальных программ-вирусов

3.3.1. В целях съема информации, ее разрушения, нарушения нормального функционирования СВТ и АС создаются специальные программы-вирусы.

3.3.2. Пути проникновения вирусов в СВТ и АС:

- проникновение вирусов на рабочие станции при использовании на рабочей станции инфицированных файлов с переносимых источников (флоппи-диски, компакт-диски и т.п.);
- заражение вирусами с помощью инфицированного программного обеспечения, полученного из Интернет и проинсталлированного на локальной рабочей станции;
- проникновение вирусов при подключении к локальной вычислительной сети (далее - ЛВС) инфицированных рабочих станций удаленных или мобильных пользователей;

- заражение вирусами с удаленного сервера, подсоединенного к ЛВС и обменивающегося инфицированными данными с ее серверами;

- распространение электронной почты, содержащей в приложениях файлы Excel и Word, инфицированные макровирусами.

3.3.3. Организация антивирусной защиты информации на объектах информатизации достигается путем:

- внедрения и применения средств антивирусной защиты информации;

- обновления баз данных средств антивирусной защиты информации;

- спланированных действий должностных лиц при обнаружении заражения информационных ресурсов программными вирусами.

3.3.4. Система антивирусной защиты должна разрабатываться с учетом особенностей конкретных ЛВС и, в общем случае, должна включать в себя:

- антивирусную защиту рабочих станций;

- антивирусную защиту серверов;

- возможность автоматического обновления антивирусных баз и версий.

3.3.5. Организация работ по антивирусной защите информации возлагается на должностных лиц, осуществляющих эксплуатацию объектов информатизации.

3.3.6. Порядок применения средств антивирусной защиты устанавливается с учетом необходимости выполнения следующих требований:

а) операторами (пользователями) информационной системы:

- периодическая проверка жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе гибких магнитных дисков перед началом работы с ними на отсутствие программных вирусов;

- внеплановая проверка магнитных носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

б) работниками подразделения, осуществляющего эксплуатацию объектов информатизации:

- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации машинных носителей информации, информационных массивов, программных средств общего и специального назначения;

- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

3.3.7. К использованию допускаются только лицензированные антивирусные средства, централизованно закупленные у разработчиков указанных средств либо их официальных дилеров.

3.3.8. При обнаружении программных вирусов пользователь обязан прекратить все работы на ПЭВМ, поставить в известность подразделение, осуществляющее эксплуатацию объектов информатизации, и совместно с его специалистами принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

При функционировании ПЭВМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

### 3.4. Защита информации от несанкционированного доступа

3.4.1. Существуют два относительно самостоятельных направления защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

Защита СВТ обеспечивается комплексом программно-технических средств. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3.4.2. Организационные меры в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны осуществляться в соответствии с требованиями Специальных требований и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам, утвержденными Решением Государственной технической комиссии при Президенте Российской Федерации от 23 мая 1997 г. № 55.

3.4.3. При обработке или хранении в АС конфиденциальной информации для ее защиты проводятся следующие организационные мероприятия:

- документальное оформление конфиденциальной информации в виде перечня сведений, подлежащих защите;
- определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
- установление и оформление правил разграничения доступа, т.е. совокупности правил доступа субъектов к данным;
- ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
- разработка системы защиты информации от НСД, включая соответствующую организационно-распорядительную документацию.

3.4.5. Защита доступа к компьютеру осуществляется программными, программно-аппаратными средствами и чисто аппаратными комплексами. Это обеспечивает:

- наличие в компьютерах только той информации и тех программ, которые необходимы работникам для повседневной деятельности;
- невозможность передачи посторонним лицам конфиденциальной информации неблагонадежными работниками;
- постоянный контроль за конфиденциальной информацией, всегда можно узнать, кто и когда к ней обратился;
- ознакомление с историей работы пользователя на компьютере;
- обеспечение защиты в незащищенных операционных системах аналогичной защите в серверной операционной системе, не повышая требований к аппаратной части компьютера;
- получение администратором сети информации о том, что происходит на компьютерах сети.

## 3.5. Защита информации от несанкционированного и непреднамеренного воздействия

3.5.1. Защита информации от несанкционированного и непреднамеренного воздействия осуществляется по следующим направлениям:

а) соблюдение порядка разработки, ввода в действие и эксплуатации объектов информатизации;

б) определение условий размещения объекта информатизации относительно границ контролируемой зоны;

в) определение технических средств и систем, предполагаемых к использованию в АС и системах связи, условий их расположения;

г) определение режимов обработки информации в АС в целом и в отдельных компонентах;

д) установление правил разграничения доступа для пользователей с целью минимизации их воздействия на программные и аппаратные средства автоматизации обработки информации;

е) повышение уровня квалификации пользователей и обслуживающего персонала;

ж) контроль, техническое обслуживание и обеспечение установленных режимов работы ТСПИ в целях предупреждения их сбоев, аварий, неисправностей;

з) применение постоянно обновляемого антивирусного программного обеспечения;

и) защита от природных и техногенных явлений и стихийных бедствий (пожары, наводнения, землетрясения, грозовые разряды, грызуны и т.п.);

к) предупреждение передачи конфиденциальной информации по открытым линиям связи и ее обработки в незащищенных АС;

л) строгое выполнение работниками установленных в организации требований по защите информации;

м) организация эффективного контроля за выполнением предусмотренных мер защиты информации;

н) использование АС в защищенном исполнении.

### 3.6. Защита информации от разглашения

3.6.1. Разглашение может происходить по формальным и неформальным каналам распространения информации.

К формальным каналам относятся деловые встречи, совещания, переговоры и тому подобные формы общения, а также обмен официальными деловыми и научными документами с использованием средств передачи официальной информации (почта, телефон, телеграф и др.).

Неформальные каналы включают:

- личное общение (встречи, переписка и др.);
- выставки, семинары, конференции и другие массовые мероприятия;
- средства массовой информации (печать, газеты, интервью, радио, телевидение и др.).

3.6.3. Условиями, способствующими неправомерному доступу к конфиденциальной информации, являются также отсутствие трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа по сплочению коллектива территориального органа (подведомственной организации).

3.6.4. Предупреждение противоправных действий с конфиденциальной информацией обеспечивается различными мерами и средствами, начиная с

создания климата осознанного отношения работников к проблеме безопасности и защиты информации.

3.6.5. Причиной разглашения конфиденциальной информации, как правило, является недостаточное знание работниками правил ее защиты и непонимание (или недопонимание) необходимости их тщательного соблюдения.

3.6.6. Правовой основой работы с работниками, допущенными к конфиденциальной информации, являются:

- наличие в служебном контракте пункта о работе со сведениями, составляющими конфиденциальную информацию;
- наличие в должностном регламенте работника пункта о том, что он работает с конфиденциальной информацией и несет ответственность за ее разглашение;
- наличие перечня сведений конфиденциального характера и инструкции по защите информации, с которыми должен быть ознакомлен работник;
- создание работникам условий для работы с информацией ограниченного доступа.