УТВЕРЖДЕНО
приказом председателя
Государственного комитета
по делам архивов
Челябинской области

«08»мая 2015г. № 62

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ КОМИТЕТЕ ПО ДЕЛАМ АРХИВОВ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано на основании требований «Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. № 912-51, федеральных законов Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Специальных требований и рекомендаций по технической защите конфиденциальной информации, утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

1.2. Под информацией, требующей защиты, понимаются сведения о Государственном комитете по делам архивов Челябинской области (далее – Государственный комитет) и его деятельности, на распространение которых в соответствии с Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188 и действующим законодательством накладываются ограничения.

1.3. Цель данного положения - на основании действующих законодательных актов и руководящих документов по защите информации создать необходимые организационно-правовые основы для эффективной защиты конфиденциальной информации.

1.4. Положение определяет порядок организации в Государственном комитете работ по разработке и эксплуатации объектов информатизации и систем защиты информации (СЗИ).

1.5. Положение предназначено для практического использования в Государственном комитете.

1.6. Требования настоящего Положения являются обязательными для исполнения во всех отделах, всеми работниками Государственного комитета.

1.7. За общее состояние и организацию работ по технической защите конфиденциальной информации отвечает заместитель председателя Государственного комитета – начальник отдела внедрения автоматизированных архивных технологий.

Ответственность за выполнение мероприятий по защите информации и эксплуатацию средств защиты информации на объектах информатизации в отделах возлагается на начальников отделов Государственного комитета, в ведении которых находятся эти объекты.

1.8. Для оказания услуг в области защиты информации могут привлекаться специализированные организации, имеющие лицензию на этот вид деятельности.

1.9. Используемые технические и программные средства защиты информации должны быть сертифицированы в соответствии с требованиями «Положения о сертификации средств защиты информации», утвержденного постановлением Правительства от 26 июня 1995 г. № 608.

1.10. Положение может уточняться и корректироваться по мере необходимости.

2. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ

2.1. Целями технической защиты конфиденциальной информации в Государственном комитете являются:

- исключение утечки конфиденциальной информации с помощью технических средств разведки;
- предотвращение несанкционированного доступа (НСД) к конфиденциальной информации, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования в системах и средствах информатизации.

2.2. Замысел достижения целей защиты информации.

Замыслом достижения целей защиты информации является обеспечение защиты информации путем строгого соблюдения действующих норм и требований ФСТЭК России (Гостехкомиссии России), созданием СЗИ объектов информатизации и принятием эффективных режимных мер, предписанных руководящими документами.

2.3. Конфиденциальная информация:

- сведения конфиденциального характера, содержащиеся в речевой информации;
- конфиденциальная информация, обрабатываемая с использованием технических средств.

2.4. Потенциальные угрозы информационной безопасности объектов.

В качестве угроз информационной безопасности объектов необходимо рассматривать:

- использование разведками иностранных государств технических средств для получения конфиденциальных сведений, перехват информации, обсуждаемой в защищаемых помещениях и циркулирующей в основных технических средствах и системах, а также воздействие на информационные ресурсы автоматизированных систем с целью разрушения, искажения и блокирования информации;
- использование криминальными структурами технических средств для получения информации, представляющей ценность в интересах планирования криминальных акций;
- несанкционированный удаленный доступ (из-за пределов контролируемых зон) в сети систем информатизации и связи объектов с целью получения информации ограниченного распространения и использования возможностей систем связи (компьютерная разведка, дистанционный доступ к

программным средствам иностранных цифровых электронных автоматических телефонных станций);

- преднамеренные действия нарушителей и злоумышленников, незаконным путем проникших на объекты посредством контактного несанкционированного доступа к элементам автоматизированных систем, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

- непреднамеренные действия персонала, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки проектирования, разработки и эксплуатации технических и программных средств автоматизированных систем.

2.5. Оценка возможностей технических средств разведки иностранных государств и криминальных структур проводится с использованием Модели иностранной технической разведки, Методик оценки возможностей иностранной технической разведки и других нормативных документов Гостехкомиссии России применительно к конфиденциальным сведениям об объектах, к информации, циркулирующей (обсуждаемой) в защищаемых помещениях и основных технических средствах и системах объектов.

2.6. Для ведения перехвата информации, циркулирующей в средствах и системах информатизации и связи объектов Государственного комитета могут использоваться следующие виды технической разведки:

- стационарная;
- портативная возимая;
- портативная носимая;
- автономная автоматическая.

2.7. Одной из возможных угроз информационным ресурсам автоматизированных систем, при определенных условиях, может являться компьютерная разведка, направленная на извлечение, систематизацию и специальную обработку открытой информации из информационно-вычислительных сетей, телекоммуникационных систем, а также информации об особенностях их построения и функционирования. Таким условием может быть несанкционированный выход с отдельных рабочих мест автоматизированных систем в глобальные информационные сети, бесконтрольное подключение к информационно-вычислительным сетям общего пользования компьютерных средств и оргтехники, находящихся на защищаемых объектах, может служить предпосылкой к утечке конфиденциальной информации.

3. ПОРЯДОК АТТЕСТАЦИИ И ВВОДА В ЭКСПЛУАТАЦИЮ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

3.1. Все объекты информатизации должны быть аттестованы на соответствие установленным нормам и требованиям по защите информации.

3.2. Аттестация по требованиям безопасности информации является необходимым условием для ввода в эксплуатацию объектов информатизации.

3.3. Аттестации подлежат объекты вычислительной техники, используемые для обработки конфиденциальной информации.

3.4. Аттестационные испытания проводятся аттестационной комиссией, формируемой аккредитованным ФСТЭК России органом по аттестации, по программе, согласованной с Государственным комитетом.

3.5. Для проведения испытаний аттестационной комиссии подготавливаются и представляются:

- технический паспорт на объект информатизации;
- акт классификации автоматизированной системы по требованиям защиты информации;
- состав технических и программных средств, входящих в автоматизированную систему (АС) (или технических средств, расположенных в выделенном помещении);
- -планы размещения основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС);
- состав и схемы размещения средств защиты информации;
- план контролируемой зоны;
- схемы прокладки линий передачи данных;
- схемы и характеристики систем электропитания и заземления объекта информатизации;
- перечень защищаемых в АС ресурсов (или конфиденциальность обсуждаемых в защищаемых помещении вопросов);
- организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам);
- инструкции пользователям и администратору безопасности информации;
- инструкции по эксплуатации средств защиты информации;
- предписания на эксплуатацию технических средств и систем;
- протоколы специальных исследований технических средств и систем;
- сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации.

3.6. Аттестационные испытания объекта информатизации проводятся до полного их завершения в соответствии с программой испытаний вне зависимости от промежуточных результатов испытаний и завершаются выдачей Аттестата соответствия.

3.7. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации, указывается в Аттестате соответствия.

3.8. Обсуждение и обработка конфиденциальной информации до окончания аттестации и приказа о вводе в эксплуатацию объектов информатизации запрещается.

4. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

4.1. Защита сведений конфиденциального характера достигается путем создания системы защиты информации, которая включает комплекс организационных, технических и программных мероприятий, направленных на закрытие технических каналов утечки информации и защиту от НСД.

4.2. Мероприятия по защите информации являются составной частью деятельности Государственного комитета, проводятся с целью закрытия возможных технических каналов утечки информации. Эти мероприятия проводятся на всех циклах создания, развития и эксплуатации используемых технических систем и средств, а также при ремонте, реконструкции и эксплуатации защищаемых помещений.

4.3. С целью закрытия возможных технических каналов утечки речевой информации рекомендуется проведение следующих мероприятий:

4.3.1. Применение организационно-режимных мероприятий:

- временное увеличение контролируемой зоны;
- закрытие дверей в защищаемые помещения между мероприятиями и в нерабочее время на ключ;
- выдача ключей от защищаемых помещений только лицу, ответственному за это помещение;
- установка и замена оборудования, мебели, ремонт в защищаемых помещениях производятся только по согласованию и под контролем начальника отдела по защите государственной тайны и мобилизационной подготовки.

4.3.2. Обеспечение необходимой звукоизоляции защищаемых помещений (закрытие акустического и виброакустического каналов утечки информации) путем:

- обивки входных дверей звукопоглощающими материалами;
- оборудования подвесных звукопоглощающих потолков со звукоизолирующим слоем;
- усиления стен и перегородок конструкциями типа «стена на откосе»;
- применения надежных шумопоглотителей для вентиляционных отверстий;
- оборудования двойных дверей с тамбуром с вибрационной развязкой дверных коробок;
- использования штор из плотной материи на окнах;
- применения звукопоглощающих материалов для покрытия стен, потолка и пола.

4.3.3. Принятие мер по закрытию электроакустического канала за счет установки в защищаемых помещениях:

- устройств телефонной связи, радиотрансляции, оповещения, сигнализации и электрочасофикации, сертифицированных по требованиям безопасности информации, либо прошедших специальные исследования, имеющие предписание на эксплуатацию;

- защищенных от утечки информации за счет электроакустических преобразований и «навязывания» оконечных устройств телефонной связи (телефонные аппараты, концентраторы, телефаксы и т.п.), включенных в городскую АТС;
- систем пожарной и охранной сигнализации, построенных только по проводной схеме сбора информации.

4.3.4. Проведение временных ограничительных мероприятий по использованию отдельных помещений для ведения переговоров, установке и использованию в них технических средств.

4.3.5. Запрещение использования радиотелефонов, оконечных устройств сотовой, пейджинговой связи, не защищенных переносных магнитофонов и других средств аудио и видеозаписи.

4.3.6. Отключение от сети телефонных и факсимильных аппаратов с автоответчиками или спикерфоном, а также телефонных аппаратов с автоматическим определителем номера.

4.3.7. Проведение специальной проверки защищаемых помещений на наличие возможно внедренных в них специальных подслушивающих устройств, по решению председателя Государственного комитета.

4.4. С целью закрытия возможных каналов утечки сведений, отнесенных к конфиденциальной информации, при их обработке и хранении в технических системах и средствах рекомендуется применение следующих мер защиты:

- использование технических средств, сертифицированных по требованиям безопасности информации;
- использование сертифицированных средств защиты информации;
- размещение трансформаторной подстанции и контура заземления технических средств внутри контролируемой зоны;
- проведение объектовых измерений в местах обработки конфиденциальной информации с оценкой эффективности и достаточности принятых мер защиты;
- предотвращение организационными мерами несанкционированного доступа к обрабатываемой информации;
- выполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- выполнение требований постановления Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», приказа Росреестра от 10.10.2011 № П/0375/11 «Об организации работы со служебной информацией ограниченного распространения в центральном аппарате Федеральной службы государственной регистрации, кадастра и картографии, ее территориальных органах»;
- выполнение положений Специальных требований и рекомендаций по технической защите конфиденциальной информации при организации обработки информации в локальных вычислительных сетях;

- выполнение требований Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- осуществление учета машинных носителей информации и их хранение в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах);
- иные меры, требования которых обязательны для выполнения в сфере защиты информации.

5. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

5.1.Председатель Государственного комитета:

- контролирует организацию работ по защите информации в Государственном комитете;
- утверждает перечень защищаемых помещений, основных технических систем и средств, также другие документы по вопросам защиты информации.

5.2 Заместитель председателя Государственного комитета – начальник отдела внедрения автоматизированных архивных технологий:

- осуществляет непосредственное руководство и координацию работ по защите информации в соответствии с руководящими документами по данному вопросу;
- совместно с начальниками отделов Государственного комитета осуществляет планирование мероприятий по защите информации, мероприятий по подготовке помещений и объектов информатизации к работе со сведениями конфиденциального характера, организовывает их выполнение и контроль их эффективности;
- разрабатывает организационно-распорядительные документы по вопросам защиты информации;
- анализирует информацию, циркулирующую в помещениях, технических системах и средствах, состояние защищенности информационных ресурсов, определяет возможные технические каналы утечки, готовит предложения по совершенствованию системы защиты;
- определяет реальную опасность перехвата информации техническими средствами разведки, несанкционированного доступа к ней, разрушения (уничтожения) и искажения, разрабатывает соответствующие меры по ее защите;
- участвует в рассмотрении и согласовании документов, определяющих пропускной и внутриобъектовый режим, разрабатывает предложения по финансированию мероприятий, связанных с защитой информации;
- незамедлительно докладывает руководителю об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также о случаях выявления попыток неправомерного доступа к сведениям, составляющим государственную или иную тайну, или попыток хищения, копирования, изменения и принимает меры пресечения;

- организует контроль состояния системы защиты информации, выполнения требований законодательства Российской Федерации по вопросам защиты информации, нормативных документов ФСТЭК России;

- в установленные сроки готовит необходимую отчетную документацию о состоянии работ по защите информации, разрабатывает предложения по дальнейшему совершенствованию системы защиты информации при использовании технических средств.

Заместитель председателя Государственного комитета – начальник отдела внедрения автоматизированных архивных технологий имеет право:

- контролировать исполнение приказов и распоряжений вышестоящих организаций и председателя Государственного комитета по вопросам сохранения конфиденциальной информации;

- требовать от начальников отделов Государственного комитета устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;

- требовать от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;

- рекомендовать запрещать эксплуатацию систем обработки и передачи информации при несоблюдении требований по защите информации;

- готовить проекты договоров на выполнение работ по защите информации со сторонними организациями, имеющими необходимые лицензии;

- вносить предложения по совершенствованию системы защиты информации.

5.3. Работник Государственного комитета, на которого возложены обязанности по защите информации:

- проводит контроль работы средств защиты информации, применяемых в Государственном комитете;

- анализирует состояние защищенности информационных ресурсов сети Государственного комитета, готовит предложения по совершенствованию систем защиты;

- принимает меры по предупреждению угроз безопасности информации, возникающих в результате случайных ошибок работников при обработке электронных документов;

- принимает участие в оценке реальной опасности утечки информации, подлежащей защите при использовании технических средств, в разработке эффективных и экономически обоснованных мер по ее защите;

- организует работу по эксплуатации системы защиты информации в автоматизированных системах обработки электронных документов;

- проводит работы по внедрению технических и программных средств защиты информации от несанкционированного доступа к ней на действующих автоматизированных системах и отдельных средствах вычислительной техники;

- распределяет между пользователями средств вычислительной техники необходимые реквизиты криптографической защиты (пароли, ключи защиты и

т.п.), формирует и распределяет между пользователями необходимые реквизиты защиты от НСД (в зависимости от системы защиты);

- проводит контроль целостности СЗИ, программного обеспечения с целью выявления несанкционированных изменений в них;
- контролирует проведение пользователями резервного копирования (архивирования) секретной информации, соблюдение мер специальной защиты при эксплуатации средств вычислительной техники (СВТ);
- принимает участие в разработке документов по обеспечению безопасности информации при эксплуатации локальной вычислительной сети (ЛВС);

- не допускает подключения к локальной сети или к СВТ нештатных блоков и устройств, не прошедших специальные исследования, не имеющих предписания на эксплуатацию;

- проводит периодический контроль СВТ, подключенных к защищаемой ЛВС, на предмет исключения несанкционированного изменения в составе, конструкции, конфигурации, размещении СВТ, а также в составе программного обеспечения;

- осуществляет контроль прав доступа работников Государственного комитета к информационным ресурсам локальной вычислительной сети;

- осуществляет контроль разграничения прав доступа к защищаемой информации на несъемных носителях информации рабочих мест пользователей;

- организует работы по выявлению возможных каналов утечки секретных сведений за счет несанкционированных доступов к информации и техническим средствам вычислительной техники (ВТ), ведет их учет;

- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток неправомерного доступа к конфиденциальной информации, или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и сообщает заместителю председателя Государственного комитета – начальнику отдела внедрения автоматизированных архивных технологий.

5.4. Работник Государственного комитета на которого возложены обязанности по защите информации имеет право:

- иметь доступ к средствам обработки и передачи информации отделов Государственного комитета, осуществлять проверки состояния защиты информации, контролировать состояние защищенности объектов информатики;

- требовать от пользователей автоматизированных систем безусловного соблюдения установленной технологии обработки электронных документов и выполнения ими требований по информационной безопасности.

5.5. Пользователи объекта ВТ обязаны:

- строго соблюдать требования по защите информации и правила эксплуатации СВТ;

- обеспечивать сохранность комплекта ПЭВМ, машинных носителей информации и целостность установленного программного обеспечения;

- знать и соблюдать установленные требования по учету, хранению и пересылке машинных, бумажных и иных носителей информации;

- применять антивирусные программы при включении СВТ или при использовании съемных машинных носителей информации;

- по окончании обработки конфиденциальной информации «обнулить» оперативную память компьютера путем перезагрузки или временного выключения ПЭВМ;

- перед началом обработки конфиденциальной информации убедиться в работе средств защиты информации (антивирусная программа);

5.6. Начальники отделов Государственного комитета:

- лично отвечают за защиту информации в отделе, сохранность машинных и иных носителей информации;

- организуют выполнение мероприятий по защите конфиденциальной информации при использовании технических средств;

- участвуют в определении правил разграничения доступа к информации в используемых системах и средствах информатизации;

- согласуют с заместителем председателя Государственного комитета – начальником отдела внедрения автоматизированных архивных технологий установку, замену и перемещение технических средств в помещениях отделов.

6. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Контроль состояния защиты информации осуществляется в целях предотвращения утечки информации по техническим каналам, несанкционированного доступа к информации, хищения технических средств и носителей информации.

6.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

6.3. Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты информации, проводится заместителем председателя Государственного комитета – начальником отдела внедрения автоматизированных архивных технологий.

6.4. Периодический контроль может осуществляться представителями ФСТЭК России, территориальных органов УФСБ России, Роскомнадзора России, отдела по защите государственной тайны Росреестра.

6.5. Допуск представителей этих органов для проведения контроля состояния защиты информации осуществляется в установленном порядке по предъявлению служебных удостоверений и предписания на право проверки, подписанного руководителем (заместителем) соответствующего органа.

6.6. Результаты проверок отражаются в техническом паспорте объекта информатизации.

6.7. Периодичность проверок объектов информатизации, где обрабатывается (обсуждается) конфиденциальная информация - 1 раз в год

и при каждом изменении состава и расположения основных технических средств и систем.

6.8. Заместитель председателя Государственного комитета – начальник отдела внедрения автоматизированных архивных технологий обязан присутствовать при всех проверках Государственного комитета по вопросам защиты информации.

6.9. По результатам проверок контролирующими органами заместитель председателя Государственного комитета – начальник отдела внедрения автоматизированных архивных технологий в десятидневный срок разрабатывает план устранения выявленных недостатков.

6.10. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

6.11. При обнаружении нарушений председатель Государственного комитета обязан принять необходимые меры по их устранению в сроки, согласованные с органом или лицом, проводившим проверку.