УТВЕРЖДЕНО
приказом председателя
Государственного комитета
по делам архивов
Челябинской области

«08» мая 2015 г. № 62

ПОЛОЖЕНИЕ
О СИСТЕМЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ КОМИТЕТЕ ПО ДЕЛАМ АРХИВОВ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение является документом, обязательным для исполнения в Государственном комитете по делам архивов Челябинской области (далее –Государственный комитет) при проведении работ по технической защите информации (не криптографическими методами), содержащей сведения, отнесенные к государственной тайне или конфиденциальной информации, от ее утечки по техническим каналам, несанкционированного доступа к информации, специальных воздействий на информацию.

Положение определяет структуру системы технической защиты информации в Государственном комитете, ее задачи, функции и финансирование мероприятий по технической защите информации.

1.2. В настоящем Положении применяются следующие основные термины, регламентированные Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»:

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

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

Техническая защита информации (ТЗИ): защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Защита информации от утечки: Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Защита информации от непреднамеренного воздействия: защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа (ЗИ от НСД): защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных

нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Объект защиты информации: Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

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

Защищаемая информационная система: информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

Угроза (безопасности информации): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Несанкционированное воздействие на информацию: воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Техника защиты информации: средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

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

Эффективность защиты информации: степень соответствия результатов защиты информации цели защиты информации.

1.3. Правовую основу работ по технической защите информации в Государственном комитете составляют Конституция Российской Федерации, Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности», Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне», Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 04.07.1996 № 85-ФЗ «Об участии в международном информационном обмене» и другие нормативные правовые акты Российской Федерации и субъекта Российской Федерации в области технической защиты информации.

1.4. Функционирование системы технической защиты информации осуществляется на основе следующих принципов:

- законности;
- разграничения полномочий федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций по обеспечению технической защиты информации;

- сочетание коллегиальности решений, принимаемых в интересах системы технической защиты информации, и полной самостоятельности предприятий, учреждений и организаций при выборе средств и способов выполнения этих решений;

- сочетания правовых, организационных и технических методов защиты информации.

1.5. Целями системы технической защиты информации являются:

- предотвращение или существенное снижение ущерба безопасности Государственному комитету с использованием методов и средств технической защиты информации;

- обеспечение условий, способствующих реализации политики Государственного комитета в сфере информационной безопасности;

- реализация единой государственной технической политики, организация и координация работ по технической защите информации;

- обеспечение условий по осуществлению безопасности информационных ресурсов, подведомственных Государственному комитету.

1.6. Основными задачами системы технической защиты информации являются:

- проведение в Государственном комитете единой государственной политики по технической защите информации;

- исключение или существенное затруднение добывания информации средствами технической разведки путем предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию с целью ее уничтожения, искажения и блокирования;

- подготовка предложений по совершенствованию правового, нормативно-методического, научно - технического и организационного обеспечения технической защиты информации в Государственном комитете;

- принятие в пределах компетенции локальных правовых документов, регулирующих отношения в области технической защиты информации в Государственном комитете;

- анализ состояния и прогнозирование источников угроз безопасности информации в Государственном комитете;

- разработка целевых программ по технической защите информационных ресурсов и средств информатизации в Государственном комитете;

- учет информационных ресурсов, систем и средств формирования, передачи, хранения, обработки и распространения информации, подлежащих технической защите;

- контроль и анализ состояния технической защиты информации в Государственном комитете;

- выявление ключевых проблем в Государственном комитете в области технической защиты информации, определение приоритетных направлений развития;

- совершенствование и развитие системы подготовки кадров в области технической защиты информации в Государственном комитете.

1.7. Основными объектами обеспечения технической защиты информации являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;
- помещения, предназначенные для ведения переговоров, в ходе которых оглашаются сведения ограниченного доступа.

1.8. Мероприятия по технической защите информации являются составной частью управленческой, научной и служебной деятельности и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности и конфиденциальности проводимых работ.

Главными направлениями работ по технической защите информации в Государственном комитете являются:

- обеспечение эффективного управления системой технической защиты информации;
- организационно - режимное обеспечение технической защиты информации, отнесенной к государственной тайне или конфиденциальной информации;
- обеспечение физической защиты объектов и средств автоматизации;
- обеспечение технической защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче ее на объектах информатизации;
- обеспечение технической защиты информации от НСД в автоматизированных информационных системах и локальных вычислительных сетях, а также от компьютерных вирусов;
- совершенствование методической базы обеспечения технической защиты информации;
- организация и проведение контроля состояния технической защиты информации;

1.10. Основными организационно-техническими мероприятиями по технической защите информации в Государственном комитете являются:

- формирование методической базы для деятельности в области технической защиты информации;
- планирование деятельности по технической защите информации;

- проведение анализа и оценки разведывательной обстановки в Государственном комитете;
- контроль эффективности мер технической защиты информации на объектах защиты;
- категорирование объектов защиты в зависимости от их важности, этапов жизненного цикла, степени секретности защищаемой информации и условий эксплуатации, а также классификация автоматизированных систем по требованиям защищенности от НСД к информации;
- разработка и внедрение технических решений по технической защите информации при создании и эксплуатации объектов информатизации;
- использование технических мер и применение средств технической защиты информации, исключающих перехват информации, передаваемой по каналам связи;
- создание и применение сертифицированных информационных и автоматизированных систем управления в защищенном исполнении;
- аттестация объектов информатизации по требованиям безопасности информации;
- сбор и анализ информации о нападении на информационные системы и принятие адекватных мер защиты;
- ведение учета информационных ресурсов.

1.11. Конкретные методы, приемы и меры технической защиты информации разрабатываются с учетом возможного ущерба в случае утечки, уничтожения, искажения и блокирования защищаемой информации, а также затрат на их реализацию.

1.12. Проведение любых мероприятий и работ с использованием защищаемой информации без принятия необходимых мер по технической защите информации не допускается.

1.13. Ответственность за организацию, своевременную реализацию эффективных мер технической защиты информации возлагается на заместителя председателя Государственного комитета – начальника отдела внедрения автоматизированных архивных технологий.

2. СИСТЕМА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Система технической защиты информации представляет собой совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

2.2. К органам технической защиты информации в Государственном комитете относятся:

- отдел внедрения автоматизированных архивных технологий, постоянно действующая техническая комиссия по защите государственной тайны (ПДТК).

2.3. Руководство работами по технической защите информации в Государственном комитете осуществляется заместителем председателя Государственного комитета – начальником отдела внедрения автоматизированных архивных технологий.

3. ОРГАНИЗАЦИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

3.1. Основными целями технической защиты информации на объектах информатизации являются:

- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки;
- сохранение возможности управления процессом обработки и пользования информацией.

3.2. Техническая защита информации на объектах информатизации осуществляется путем:

- исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации, а также информации, передаваемой по каналам связи;
- предотвращения специальных воздействий, вызывающих уничтожение, искажение и блокирование информации или сбои в работе средств информатизации;
- выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок;
- предотвращения утечки акустической речевой информации из помещений и объектов.

3.3. Защищаемая информация должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

Для оценки готовности объектов информатизации к обработке (передаче) защищаемой информации проводится аттестация указанных объектов в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации. При положительных результатах аттестации выдается аттестат соответствия на обработку защищаемой информации.

Аттестация объектов информатизации осуществляется аккредитованными установленным порядком органами по аттестации.

4. КОНТРОЛЬ СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Контроль состояния технической защиты информации (далее - контроль) осуществляется в целях оценки организации технической защиты информации, своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, оценки защиты ее от технических разведок.

Контроль заключается в проверке выполнения требований законодательства Российской Федерации по вопросам технической защиты информации, нормативно-методических и руководящих документов ФСТЭК России, Роскомнадзора, а также в оценке достаточности принимаемых мер технической защиты информации.

4.2. Основными задачами контроля являются:

- оценка деятельности органов власти по руководству и координации работ в области технической защиты информации в пределах их компетенции;
- выявление технических каналов утечки информации об объектах защиты, каналов несанкционированного доступа к информации и специальных воздействий на информацию, анализ и инструментальная оценка возможностей технических разведок по получению информации;
- оценка эффективности проводимых мер по технической защите информации;
- выявление и анализ нарушений установленных норм и требований по технической защите информации и принятие оперативных мер по пресечению выявленных нарушений;
- разработка рекомендаций по устранению выявленных недостатков в организации и состоянии работ по технической защите информации;
- проверка устранения недостатков, выявленных в результате контроля.

4.3. Контроль состояния технической защиты информации в субъекте Российской Федерации организуется в соответствии с действующими нормативными правовыми актами Российской Федерации и субъекта Российской Федерации.

4.4. Контроль технической защиты информации в Государственном комитете осуществляется отделом внедрения автоматизированных архивных технологий. На него возлагается проведение регулярного контроля состояния технической защиты информации (порядка функционирования средств технической защиты информации, соблюдения установленных режимов работы объектов информатизации, выполнения установленных мер технической защиты информации, в том числе от НСД).

4.5. Невыполнение требований руководящих и нормативно-методических документов по технической защите информации, составляющей государственную тайну, является нарушением норм и требований по ТЗИ.

4.6. Защита информации считается эффективной, если принятые меры соответствуют требованиям руководящих и нормативных документов по технической защите информации.