ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В СЛУЖЕБНЫХ ПОМЕЩЕНИЯХ

Общие технические требования

СТ РК 1700-2007

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН ТОО «Специальное конструкторско-технологическое бюро «ГРАНИТ»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 24 декабря 2007 г. № 691

3 СРОК ПЕРВОЙ ПРОВЕРКИ 2012 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

4 В настоящем стандарте реализованы нормы Законов Республики Казахстан Об информатизации от 11.01.2007 г. № 217-III, О государственных секретах от 15.03.99 г. № 349-1, О национальной безопасности Республики Казахстан от 26.06.98 г. № 233-I и Постановления Правительства Республики Казахстан «Об обязательном подтверждении соответствия продукции в Республике Казахстан» от 20.04.2005 г. № 367

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Нормативные документы по стандартизации», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Нормативные документы по стандартизации». В случае пересмотра (изменения, замены) или отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячно издаваемом информационном указателе «Нормативные документы по стандартизации»

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В СЛУЖЕБНЫХ ПОМЕЩЕНИЯХ

Общие технические требования

Дата введения 2009.01.01

1 Область применения

Настоящий стандарт устанавливает требования к организации технической защиты речевой информации в служебных помещениях, в которых проводится работа с защищаемой информацией, в том числе с государственными секретами, и устанавливает классификацию технических каналов утечки, методы защиты речевой информации и требования к комплексу средств защиты речевой информации.

Положения стандарта применяются государственными органами и другими юридическими и физическими лицами, допущенными к работе с государственными секретами, в целях защиты интересов национальной безопасности Республики Казахстан.

Настоящий стандарт не рассматривает требования к процедурам и техническим средствам, применяемым для выявления каналов утечки речевой информации за счет устройств перехвата информации, внедряемых в служебные помещения, расположенное в них оборудование и линии (каналы) связи, а также методы защиты от этих и других, искусственно организуемых каналов утечки информации в процессе эксплуатации служебного помещения.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 34.005-2002 Информационная технология. Основные термины и определения.

СТ РК 34.013-2002 Информационная технология. Защита информации от утечки по каналу побочных электромагнитных излучений и наводок при ее обработке на средствах вычислительной техники.

СТ РК 34.026-2006 Защита информации. Термины и определения.

СТ РК ИСО/МЭК 17799-2006 Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации.

СТ РК ГОСТ Р 50571.22-2006 Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации.

СТ РК ГОСТ Р 50739-2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов по указателю «Нормативные документы по стандартизации», составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины, установленные в СТ РК 34.005 и СТ РК 34.026, а также следующие термины с соответствующими определениями:

3.1 **Активные методы защиты:** Методы защиты информации, основанные на создании маскирующих помех источников излучений опасных сигналов.

3.2 **Анализ рисков:** Процесс определения угроз безопасности информационных систем и отдельных ее элементов, определения их характеристик и потенциального ущерба, а также контрмер.

3.3 **Вспомогательные технические средства:** Технические средства, непосредственно не участвующие в обработке секретной информации, но используемые совместно с основными техническими средствами и находящиеся в зоне электромагнитного поля основных технических средств.

Примечание – К вспомогательным техническим средствам относятся технические средства открытой телефонной, громкоговорящей связи; системы пожарной и охранной сигнализации, электрификации, радиофикации; электробытовые приборы.

3.4 **Данные:** Информация, представленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека или автоматическими средствами.

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

3.6 **Контролируемая зона:** Минимальное расстояние вокруг объекта, в пределах которого исключается неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

3.7 **Оборудование информационных технологий:** Любое оборудование, выполняющее функцию, связанную с вводом, хранением, отображением, поиском, передачей, обработкой, управлением или коммутацией данных и речевой информации (сообщений связи).

3.8 **Опасный сигнал:** Сигнал, несущий секретную информацию, появляющийся в цепях, не предназначенных для передачи секретной информации.

3.9 **Основные технические средства:** Средства вычислительной техники, средства связи, звукозаписи, звукоусиления и звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекционная аппаратура, системы электрооборудования и другие средства и системы, используемые для обработки секретной информации.

3.10 **Пассивные методы защиты:** Методы защиты информации, основанные на принципах локализации, ограничении (фильтрации) и отключении источников излучений опасных сигналов.

3.11 **Профиль защиты:** Документ, описывающий задачи обеспечения информационной безопасности в терминах функциональных требований и требований гарантированности.

3.12 **Служебное помещение:** Специальное помещение, предназначенное для регулярного проведения совещаний, собраний, бесед и других мероприятий закрытого характера.

3.13 **Техническое задание:** Исходный технический документ заказчика на выполнение опытно-конструкторской (научно-исследовательской) работы, устанавливающий комплекс требований к содержанию, объему и срокам выполнения работы по созданию (модернизации) изделия.

3.14 **Угрозы информационной безопасности:** Совокупность причин, условий и

факторов, создающих опасность объектам информационной безопасности, реализация которых может повлечь нарушение прав, свобод и законных интересов юридических и физических лиц в информационных процессах.

4 Сокращения

В настоящем стандарте применены следующие сокращения:
ВТС – вспомогательные технические средства.
ЗИ – защита информации.
ИБ – информационная безопасность.
КСЗ – комплекс средств защиты.
ОИТ – оборудование информационных технологий.
ОТС– основные технические средства.
ПЭМИН - побочные электромагнитные излучения и наводки.
СВТ – средства вычислительной техники.
СП – служебное помещение.
ТЗ – техническое задание.
ТСЗИ – технические средства защиты информации.

5 Общие положения

5.1 Для организации технической защиты информации в служебных помещениях, сами СП и СВТ, находящиеся в них, должны быть категорированы в соответствии с требованиями нормативных документов [1], [2]. Категория СП определяется исходя из максимального грифа секретности речевой информации и информации (данных), обрабатываемой с помощью СВТ, находящихся в СП.

5.2 Проведение мероприятий секретного характера и обработка защищаемой информации разрешается только в СП, аттестованных в установленном порядке.

Решение о необходимости аттестации принимает и несет ответственность за нее руководитель организации, в ведении которого находится СП.

В процессе аттестации для каждого СП должен рассматриваться набор внутренних требований, которые формулируются по результатам анализа рисков и учитывают специфику и особенности среды функционирования аттестуемого СП.

Аттестация СП может не проводиться, если объект, в котором расположено СП, имеет Аттестат соответствия, которым подтверждается, что аттестованный объект соответствует требованиям стандартов и (или) иных нормативных документов по информационной безопасности, утвержденных уполномоченным государственным органом по защите государственных секретов и обеспечению информационной безопасности в установленном порядке.

5.3 Находящееся в СП ОИТ, как правило, а ТСЗИ в обязательном порядке, должны иметь сертификаты соответствия требованиям информационной безопасности, выдаваемые аккредитованными органами по подтверждению соответствия, или предписания на эксплуатацию по требованиям информационной безопасности и (или) противодействию техническим средствам разведки [2].

Если указанное ОИТ не имеет сертификатов соответствия или предписаний на эксплуатацию, необходимость в их получении определяется органом по аттестации на этапе предварительного ознакомления с аттестуемым объектом.

5.4 Техническая защита информации в СП реализуется техническими средствами защиты, исключающими утечку информации за пределы контролируемой зоны.

Совокупность всех ТСЗИ составляет комплекс средств защиты СП.

Поставщики и производители КСЗ, предназначенных для защиты госсекретов, должны иметь лицензию на право проведения работ в области ЗИ. Лицензирование организаций осуществляется в порядке, установленном [3].

5.5 Границами контролируемой зоны для СП являются его ограждающие конструкции (стены, окна, двери, пол, потолок). Границы контролируемой зоны могут расширяться, если соседние помещения, помещения сверху и снизу, помещения расположенные напротив окон и дверей имеют одинаковую (или выше) категорию секретности с защищаемым СП. Основное условие при расширении границ – контролируемая зона должна быть сплошной, без промежутков.

5.6 Технические требования к КСЗ задаются в техническом задании на его разработку. ТЗ на разработку КСЗ, предназначенного для защиты государственных секретов, должно в обязательном порядке согласовываться с уполномоченным государственным органом по защите государственных секретов и информационной безопасности

5.7 КСЗ должен быть заказан, разработан, изготовлен и смонтирован с учетом требований по электромагнитной совместимости, помехозащищенности и защите информации от утечки по каналам, представляющим угрозу безопасности информации.

Функционирование КСЗ не должно создавать помех в условиях его совместной работы с ОТС и ОИТ, а также с аппаратурой другого назначения (ВТС), которая может быть использована в служебном помещении или на объекте в целом.

Оборудование, установленное в СП, должно быть заземлено в соответствии с требованиями СТ РК ГОСТ Р 50571.22.

5.8 КСЗ СП должен предусматривать решение следующих задач:

- предотвращение утечки защищаемой речевой информации, циркулирующей в СП;
- предотвращение утечки защищаемой речевой информации и данных, передаваемых по линиям (каналам) связи с помощью технических средств;
- предотвращение утечки защищаемой речевой информации и данных за счет побочных электромагнитных излучений и наводок;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в СП защищаемой информации;
- организацию физической защиты и допуска в СП;
- осуществление контроля функционирования КСЗ.

5.9 Разрешительная система допуска должна обеспечивать выполнение основных положений правил разграничения доступа, установленных СТ РК ИСО/МЭК 17799.

5.10 Физическая защита предполагает оборудование защитных барьеров и контроль проникновения в СП. Требования к физической защите СП формируются исходя из важности обрабатываемой в нем информации (данных), и определяются нормативными документами уполномоченного государственного органа по защите государственных секретов и обеспечению информационной безопасности [1].

5.11 Допускается не оборудовать СП КСЗ, если объект, в котором находится СП, оборудован средствами групповой защиты от утечки информации и на объект имеется действующий Аттестат соответствия.

6 Технические требования

6.1 Классификация каналов утечки речевой информации

По характеру утечки речевой информации технические каналы подразделяются на основные типы (группы), приведенные в таблице 1.

Таблица 1 – Каналы утечки речевой информации и их краткое описание

Канал утечки информации	Описание
Акустический	Перенос энергии речевых сигналов через колебания воздушной среды. Утечка информации может осуществляться за счет слабой акустической изоляции (наличие щелей в стенах, вентиляционные каналы).
Виброакустический	Перенос энергии речевых сигналов через колебания воздушной среды на ограждающие конструкции. Утечка информации может осуществляться за счет колебаний ограждающих строительных конструкций помещения (стены, оконные стёкла) и инженерных коммуникаций (трубопроводы газо- и водоснабжения, канализации, отопления).
Оптикоакустический	Перенос энергии речевых сигналов через колебания воздушной среды на источники оптического, ультрафиолетового и инфракрасного излучения. Утечка информации может осуществляться за счет модуляции уровня свечения.
Электроакустический	Перенос энергии речевых сигналов через колебания воздушной среды на электронные устройства, способные преобразовывать акустические сигналы в электрические (например, за счёт пьезоэлектрического, электродинамического или трибоэлектрического эффекта, либо путём модуляции сигналов ВЧ-навязывания). Съем информации возможен путём анализа сигналов в проводных линиях, проходящих (выходящих) через защищаемое СП.
ПЭМИН	Утечка информации за счет модуляции опасным сигналом электромагнитных полей, образующихся при работе ОИТ или создаваемых внешним высокочастотным облучением.

6.2 Методы защиты речевой информации

6.2.1 Защита информации от утечки по акустическим каналам

6.2.1.1 Пассивные методы ЗИ от утечки по акустическим каналам должны обеспечивать ослабление энергии речевых сигналов до величин, обеспечивающих невозможность их выделения специальными средствами на фоне естественных шумов за пределами контролируемой зоны путем звукоизоляции помещений, способствующей локализации источников акустических сигналов внутри них.

Звукоизоляция СП достигается применением звукоизолирующих материалов при отделке СП, герметизацией зазоров и щелей в ограждающих конструкциях, установкой акустических фильтров и созданием интерьера СП, способствующего локализации источников акустических сигналов.

6.2.1.2 Активные методы ЗИ от утечки по акустическим каналам должны

обеспечивать создание акустических маскирующих пространственных помех в целях уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения опасных сигналов специальными средствами.

Активные методы ЗИ от утечки по акустическим каналам реализуются путём использования генераторов маскирующих акустических помех, уровень излучения которых должен превышать уровень речевых акустических сигналов.

6.2.2 Защита информации от утечки по виброакустическим каналам

6.2.2.1 Пассивные методы ЗИ от утечки по виброакустическим каналам должны обеспечивать ослабление энергии речевых сигналов до величин, обеспечивающих невозможность их выделения специальными средствами на фоне естественных шумов за пределами контролируемой зоны путем виброзвукоизоляции помещений, способствующей локализации источников акустических сигналов внутри них.

Виброизоляция СП достигается применением демпфирующих и виброзвукопоглащающих материалов при установке ограждающих конструкций и инженерных коммуникаций, развязкой трубопроводов газо- и водоснабжения, канализации, отопления, специальной конструкцией рам окон и рам, гасящей колебания оконных стекол.

6.2.2.2 Активные методы ЗИ от утечки по виброакустическим каналам должны обеспечивать создание виброакустических маскирующих пространственных помех в целях уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения опасных сигналов специальными средствами.

Активные методы ЗИ от утечки по виброакустическим каналам реализуются путём использования виброакустичеких генераторов маскирующих помех, уровень излучения которых должен превышать уровень речевых виброакустических сигналов.

6.2.3 Защита информации от утечки по оптикоакустическим каналам

6.2.3.1 Пассивные методы ЗИ от утечки по оптикоакустическим каналам должны обеспечивать ослабление энергии оптических сигналов до величин, обеспечивающих невозможность их выделения специальными средствами на фоне естественных шумов за пределами контролируемой зоны путем светоизоляции помещений, способствующей локализации источников оптических сигналов внутри них.

6.2.3.2 Активные методы ЗИ от утечки по оптикоакустическим каналам должны обеспечивать стабилизацию уровня свечения источников оптического, ультрафиолетового и инфракрасного излучения до величин, обеспечивающих невозможность выделения опасных сигналов специальными средствами на фоне аналогичных излучений за пределами контролируемой зоны.

Стабилизация уровня свечения источников излучения опасных сигналов достигается:

- путем размещения источников излучений в звукоизолирующих светопрозрачных экранах (абажурах, плафонах), способствующих снижению модуляции уровня свечения акустическими речевыми сигналами;
- путем применения светопоглащающих фильтров (пленок, стекол) на окнах СП;
- фоновой засветки окон СП в полосе частот, превышающей полосу частот излучения источников опасных сигналов.

6.2.4 Защита информации от утечки по электроакустическим каналам

6.2.4.1 Пассивные методы ЗИ от утечки по электроакустическим каналам должны обеспечивать исключение (ослабление) проникновения опасных сигналов в линии связи, цепи электропитания, радиотрансляционную линию и линию пожарно-охранной сигнализации, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность выделения опасных сигналов специальными средствами на фоне естественных шумов.

Незадействованные цепи кабелей (проводных линий), проходящих (выходящих) через СП должны быть замкнуты накоротко и заземлены в пределах контролируемой зоны.

Пассивная защита опасных сигналов достигается применением следующих технических средств:

- средств фильтрации (ослабления) опасных сигналов, в том числе сигналов высокочастотного навязывания;
- средств отключения преобразователей (источников) опасных сигналов, имеющих способность преобразовывать акустические колебания в электрические. Средства отключения преобразователей (источников) опасных сигналов могут оборудоваться средствами контроля параметров линий связи;
- экранирующих конструкций для преобразователей (источников) опасных сигналов, имеющих способность преобразовывать акустические колебания в электрические.

6.2.4.2 Активные методы ЗИ от утечки по электроакустическим каналам должны обеспечивать:

- создание маскирующих электромагнитных помех в посторонних проводниках, линиях связи и соединительных линиях ОИТ в целях уменьшения отношения сигнал/шум на границе контролируемой зоны, до величин, обеспечивающих невозможность выделения опасных сигналов специальными средствами;
- создание маскирующих электромагнитных помех в цепях электропитания в целях уменьшения отношения сигнал/шум на границе контролируемой зоны, до величин, обеспечивающих невозможность выделения опасных сигналов специальными средствами.

Активные методы ЗИ от утечки по проводным каналам связи реализуются путём использования генераторов маскирующих помех линейного зашумления.

6.2.5 Защита информации от утечки по каналу ПЭМИН

6.2.5.1 Основными пассивными методами защиты опасных сигналов по каналу ПЭМИН является экранирование преобразователей (источников) опасных сигналов и токоподводящих цепей, установка в линию телефонных фильтров, отключение преобразователей (источников) опасных сигналов.

6.2.5.2 Активные методы ЗИ по каналу ПЭМИН должны обеспечивать создание маскирующих пространственных помех в целях уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения опасных сигналов специальными средствами.

Активные методы ЗИ от утечки по каналам ПЭМИН реализуются путём использования генераторов маскирующих помех пространственного зашумления, уровень излучения которых должен превышать уровень ПЭМИН.

6.3 Требования по составу КСЗ

Состав КСЗ определяется на основе требований к ЗИ, анализа реальных угроз ИБ, вероятностью их осуществления и разработанного профиля защиты информации для конкретного служебного помещения.

Допустимые затраты на КСЗ должны соотноситься с ценностью защищаемой информации, подвергаемой риску, а также с ущербом, который может быть нанесен организации из-за реализации угроз.

6.4 Эксплуатация КСЗ

6.4.1 Эксплуатация КСЗ СП должна быть возложена на должностное лицо (подразделение) приказом руководителя организации.

Все ситуации, связанные с функционированием КСЗ, и события, связанные с нарушением режима ИБ, должны регистрироваться в контрольном журнале.

В контрольном журнале отмечается:

- дата и время включения и выключения КСЗ;
- дата и время проведения технического обслуживания ТСЗИ, проверку их параметров (в том числе инструментальных);
- выявленные попытки доступа к защищаемой информации, в том числе путем воздействия на ТСЗИ;
- прочие события, потенциально опасные с точки зрения нарушения режима ИБ.

6.4.2 Коммутационные, распределительные и согласующие устройства ОИТ, а также ТСЗИ, находящиеся в СП, должны быть опечатаны. Факт опечатывания фиксируется в соответствующем журнале с указанием номера печати, даты опечатывания, фамилии и подписи должностного лица.

6.4.3 В процессе эксплуатации КСЗ должна быть организована периодическая проверка уровня защищенности информации и правильность функционирования механизмов безопасности.

Периодичность контроля устанавливается в зависимости от категории СП в соответствии с требованиями нормативных документов [1].

6.4.4 При изменении условий функционирования СП (состава ОТС и ВТС, их размещения и т. п.) должны быть проведены дополнительные мероприятия, начиная с этапа анализа специальных требований и рекомендаций по ЗИ.

Приложение
(справочное)

Библиография

[1] Инструкция по обеспечению режима секретности в Республике Казахстан, от 14.03.2000 г. № 390-16с.

[2] Инструкция по обеспечению режима секретности при обработке сведений, составляющих государственные секреты, с применением средств вычислительной техники, утверждена Приказом Председателя Агентства Республики Казахстан по защите государственных секретов от 29.01.2001 г. № 2.

[3] Правила лицензирования деятельности по технической защите государственных секретов Республики Казахстан, утверждены Постановлением Правительства Республики Казахстан от 14.12.2000 г. № 1842.

УДК 681.3 **МКС** 35.080 **КПВЭД** 33.3

Ключевые слова: информационная безопасность, комплекс средств защиты информации, активные средства защиты информации, пассивные средства защиты информации.

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы
Есіл өзенінің сол жақ жағалауы, Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074