ДСТУ 3396.1—96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УКРАИНЫ

Защита информации

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Порядок проведения работ

Издание официальное

Киев
ГОССТАНДАРТ УКРАИНЫ
1997

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАН И ВНЕСЕН Государственной службой Украины по вопросам технической защиты информации

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Госстандарта Украины от 19 декабря 1996 г. № 51

3 В настоящем стандарте реализованы нормы Законов Украины «Об информации», «О государственной тайне», «О защите информации в автоматизированных системах»

4 ВВЕДЕН ВПЕРВЫЕ

5 РАЗРАБОТЧИКИ: А. Баранов, канд. техн. наук, В. Дюпин, А. Новиченко, В. Гелевера, И. Арутюнова

СОДЕРЖАНИЕ

ДСТУ 3396.1—96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УКРАИНЫ

ЗАЩИТА ИНФОРМАЦИИ
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Порядок проведения работ

ЗАХИСТ ІНФОРМАЦІЇ
ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ
Порядок проведення робіт

INFORMATION PROTECTION
TECHNICAL PROTECTION OF INFORMATION
Order of carrying out the works

Дата введения 1997—07—01

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт устанавливает требования к порядку проведения работ по технической защите информации (ТЗИ).

Требования стандарта обязательны для предприятий и учреждений всех форм собственности и подчинения, граждан-субъектов предпринимательской деятельности, органов государственной власти, органов местного самоуправления, войсковых частей всех воинских формирований, представительств Украины за рубежом, которые владеют, пользуются и распоряжаются информацией, подлежащей технической защите.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте приведены ссылки на следующий стандарт:

ДСТУ 3396.0—96 Защита информации. Техническая защита информации. Основные положения.

Издание официальное

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Информация с ограниченным доступом (ИсОД) в процессе информационной деятельности (ИД), основными видами которой является получение, использование, распространение и хранение ИсОД может подвергаться воздействию угроз ее безопасности (далее — угроза), в результате чего может произойти утечка или нарушение целостности информации.

Подверженность ИсОД воздействию угроз определяет ее уязвимость.

Способность системы защиты информации противостоять воздействию угроз определяет защищенность ИсОД.

3.2 Возможны следующие варианты постановки задач защиты информации:

— достижение необходимого уровня защиты ИсОД при минимальных затратах и допустимом уровне ограничений видов ИД;

— достижение наиболее возможного уровня защиты ИсОД при допустимых затратах и заданном уровне ограничений видов ИД;

— достижение максимального уровня защиты ИсОД при необходимых затратах и минимальном уровне ограничений видов ИД.

Защита информации, не являющейся государственной тайной, обеспечивается, как правило, использованием первого или второго варианта.

Защита информации, составляющей государственную тайну, обеспечивается, как правило, использованием третьего варианта.

3.3 Содержание и последовательность работ по противодействию угрозам или их нейтрализации должны соответствовать указанным ДСТУ 3396.0—96 этапам функционирования системы защиты информации и заключаются в:

— проведении обследования предприятия, учреждения, организации (далее — предприятие);

— разработке и реализации организационных, первичных технических, основных технических мер с использованием средств обеспечения ТЗИ (приложение А);

— приемке работ по ТЗИ;

— аттестации средств (систем) обеспечения информационной деятельности на соответствие требованиям нормативных документов системы ТЗИ (НД ТЗИ).

3.4 Порядок проведения работ по ТЗИ или отдельных их этапов устанавливается приказом (распоряжением) руководителя предприятия.

Работы должны выполняться силами предприятия под руководством специалистов по ТЗИ.

Для участия в работах, оказания методической помощи, оценки полноты и качества реализации мер защиты могут привлекаться специалисты по ТЗИ других организаций, имеющих лицензию уполномоченного Кабинетом Министров Украины органа.

4 ОРГАНИЗАЦИЯ ПРОВЕДЕНИЯ ОБСЛЕДОВАНИЯ

4.1 Целью обследования предприятия является изучение его ИД, определение объектов защиты — ИсОД, выявление угроз, их анализ и построение частной модели угроз.

4.2 Обследование должно быть проведено комиссией, состав которой определяется ответственным за ТЗИ лицом и утверждается приказом руководителя предприятия.

4.3 В ходе обследования необходимо:

— провести анализ условий функционирования предприятия, его расположения на местности (ситуационного плана) для определения возможных источников угроз;

— исследовать средства обеспечения ИД, имеющие выход за пределы контролируемой территории;

— изучить схемы средств и систем жизнеобеспечения предприятия (электропитания, заземления, автоматизации, пожарной и охранной сигнализации), а также инженерных коммуникаций и металлоконструкций;

— исследовать информационные потоки и технологические процессы обработки информации;

— определить наличие и техническое состояние средств обеспечения ТЗИ;

— проверить наличие на предприятии нормативных документов, обеспечивающих функционирование системы защиты информации, организацию проектирования строительных работ с учетом требований по ТЗИ, а также нормативной и эксплуатационной документации, обеспечивающей ИД;

— выявить наличие транзитных, незадействованных (воздушных, настенных, наружных и заложенных в канализацию) кабелей, цепей и проводов;

— определить технические средства и системы, применение которых не обосновано служебной или производственной необходимостью и которые подлежат демонтажу;

— определить технические средства, требующие переоборудования (перемонтажа) и установки средств ТЗИ.

4.4 По результатам обследования следует составить акт, который должен быть утвержден руководителем предприятия.

4.5 Материалы обследования необходимо использовать при разработке частной модели угроз, которая должна включать:

— генеральный и ситуационный планы предприятия, схемы расположения средств и систем обеспечения ИД, а также инженерных коммуникаций, выходящих за пределы контролируемой территории;

— схемы и описания каналов утечки информации, каналов специального воздействия и путей несанкционированного доступа к ИсОД;

— оценку предполагаемого ущерба от реализации угроз.

5 ОРГАНИЗАЦИЯ РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

5.1 На основании материалов обследования и частной модели угроз необходимо определить главные задачи защиты информации и составить техническое задание (ТЗ) на разработку системы защиты информации.

5.2 ТЗ должно включать основные разделы:

— требования к системе защиты информации;

— требования к составу проектной и эксплуатационной документации;

— этапы выполнения работ;

— порядок внесения изменений и дополнений к разделам ТЗ;

— требования к порядку проведения испытаний системы защиты

5.3 Основой функционирования системы защиты информации является план ТЗИ, который должен включать следующие документы:

— перечень распорядительных, организационно-методических, НД ТЗИ и указания по их применению;

— инструкции о порядке реализации организационных, первичных технических и основных технических мер защиты;

— инструкции, устанавливающие обязанности, права и ответственность персонала;

— календарный план ТЗИ.

5.4 ТЗ и план ТЗИ разрабатывают специалисты по ТЗИ, согласуют с заинтересованными подразделениями (организациями). Утверждает их руководитель предприятия.

6 РЕАЛИЗАЦИЯ ОРГАНИЗАЦИОННЫХ МЕР ЗАЩИТЫ

6.1 Организационные меры защиты информации — комплекс административных и ограничительных мер, направленных на оперативное решение задач защиты путем регламентации деятельности персонала и порядка функционирования средств (систем) обеспечения ИД и средств (систем) обеспечения ТЗИ.

6.2 В процессе разработки и реализации организационных мер необходимо:

— определить частные задачи защиты ИсОД;

— обосновать структуру и технологию функционирования системы защиты информации;

— разработать и внедрить правила реализации мер ТЗИ;

— определить и установить права и обязанности подразделений и лиц, участвующих в обработке ИсОД;

— приобрести средства обеспечения ТЗИ и нормативные документы и обеспечить ими предприятие;

— установить порядок внедрения защищенных средств обработки информации, программных и технических средств защиты информации, а также средств контроля ТЗИ;

— установить порядок контроля функционирования системы защиты информации и ее качественных характеристик;

— определить зоны безопасности информации;

— установить порядок проведения аттестации системы технической защиты информации, ее элементов и разработать программы аттестационных испытаний;

— обеспечить управление системой защиты информации.

6.3 Оперативное решение задач ТЗИ достигается организацией управления системой защиты информации, для чего необходимо:

— изучать и анализировать технологию прохождения ИсОД в процессе ИД;

— оценивать подверженность ИсОД воздействию угроз в конкретный момент времени;

— оценивать ожидаемую эффективность применения средств обеспечения ТЗИ;

— определять (при необходимости) дополнительную потребность в средствах обеспечения ТЗИ;

— осуществлять сбор, обработку и регистрацию данных, относящихся к ТЗИ;

— разрабатывать и реализовывать предложения по корректировке плана ТЗИ в целом или отдельных его элементов.

7 РЕАЛИЗАЦИЯ ПЕРВИЧНЫХ ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ

7.1 В процессе реализации первичных технических мер защиты требуется обеспечить:

— блокирование каналов утечки информации;

— блокирование несанкционированного доступа к информации или ее носителям;

— проверку исправности и работоспособность технических средств обеспечения ИД.

7.2 Блокирование каналов утечки информации может осуществляться:

— демонтажом технических средств, линий связи, сигнализации и управления, энергетических сетей, использование которых не связано с жизнеобеспечением предприятия и обработкой ИсОД;

— удалением отдельных элементов технических средств, являющихся средой распространения полей и сигналов, из помещений, где циркулирует ИсОД;

— временным отключением технических средств, не участвующих в обработке ИсОД, от линий связи, сигнализации, управления и энергетических сетей;

— применением способов и схемных решений по защите информации, не нарушающих основные технические характеристики средств обеспечения ИД.

7.3 Блокирование несанкционированного доступа к информации или ее носителям может осуществляться:

— созданием условий работы в пределах установленного регламента;

— исключением возможности использования не прошедших проверку (испытания) программных, программно-аппаратных средств.

7.4 Проверку исправности и работоспособности технических средств и систем обеспечения ИД необходимо проводить в соответствии с эксплуатационными документами.

Выявленные неисправные блоки и элементы могут способствовать утечке или нарушению целостности информации и подлежат немедленной замене (демонтажу).

8 РЕАЛИЗАЦИЯ ОСНОВНЫХ ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ

8.1 В процессе реализации основных технических мер защиты требуется:

— установить средства выявления и индикации угроз и проверить их работоспособность;

— установить защищенные средства обработки информации, средства ТЗИ и проверить их работоспособность;

— применить программные средства защиты в средствах вычислительной техники, автоматизированных системах, осуществить их функциональное тестирование и тестирование на соответствие требованиям защищенности;

— применить специальные инженерно-технические сооружения, средства (системы).

8.2 Выбор средств обеспечения ТЗИ обуславливается фрагментарным или комплексным способом защиты информации.

Фрагментарная защита обеспечивает противодействие определенной угрозе.

Комплексная защита обеспечивает одновременное противодействие множеству угроз.

8.3 Средства выявления и индикации угроз применяются для сигнализации и оповещения владельца (пользователя, распорядителя) ИсОД об утечке информации или нарушении ее целостности.

8.4 Средства ТЗИ применяются автономно или совместно с техническими средствами обеспечения ИД для пассивного или активного скрытия ИсОД.

Для пассивного скрытия применяются фильтры-ограничители, линейные фильтры, специальные абонентские устройства защиты и электромагнитные экраны.

Для активного скрытия применяются узкополосные и широкополосные генераторы линейного и пространственного зашумления.

8.5 Программные средства применяются для обеспечения:

— идентификации и аутентификации пользователей, персонала и ресурсов системы обработки информации;

— разграничения доступа пользователей к информации, средствам вычислительной техники и техническим средствам автоматизированных систем;

— целостности информации и конфигурации автоматизированных систем;

— регистрации и учета действий пользователей;

— маскирования обрабатываемой информации;

— реагирования (сигнализации, отключения, приостановки работ, отказа в запросе) на попытки несанкционированных действий.

8.6 Специальные инженерно-технические сооружения, средства и системы применяются для оптического, акустического, электромагнитного и другого экранирования носителей информации.

К ним относятся специально оборудованные светопроницаемые, технологические и санитарно-технические проемы, а также специальные камеры, перекрытия, навесы, каналы и т. п.

8.7 Размещение, монтаж и прокладку специальных инженерно-технических средств и систем, в том числе систем заземления и электропитания средств обеспечения ИД, следует осуществлять в соответствии с требованиями НД ТЗИ.

8.8 Технические характеристики, порядок применения и проверки средств обеспечния ТЗИ приводятся в соответствующей эксплуатационной документации

9 ПРИЕМКА, ОПРЕДЕЛЕНИЕ ПОЛНОТЫ И КАЧЕСТВА РАБОТ

9.1 По результатам выполнения рекомендаций акта обследования и реализации мер защиты ИсОД следует составить в произвольной форме акт приемки работ по ТЗИ, который должен быть подписан исполнителем работ, лицом, ответственным за ТЗИ, и утвержден руководителем предприятия.

Примечание. При необходимости акт приемки работ может быть согласован с заинтересованными организациями

9.2 Для определения полноты и качества работ по ТЗИ следует провести аттестацию. Аттестация выполняется организациями, которые имеют лицензию на право деятельности в области ТЗИ.

9.3 Объектами аттестации являются системы обеспечения ИД, отдельные их элементы, в которых циркулирует информация, подлежащая технической защите.

9.4 В ходе аттестации требуется:

— установить соответствие аттестуемого объекта требованиям ТЗИ;

— оценить качество и надежность мер защиты информации;

— оценить полноту и достаточность технической документации для объекта аттестации;

— определить необходимость внесения изменений и дополнений в организационно-распорядительные документы.

Порядок аттестации устанавливается НД ТЗИ.

ПРИЛОЖЕНИЕ А
(справочное)

Состав средств обеспечения технической защиты информации

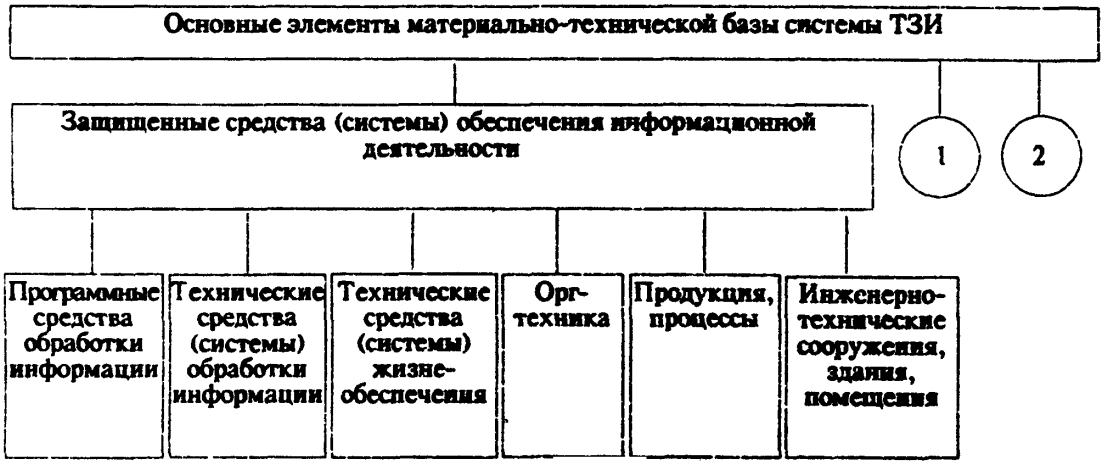

Рисунок А. 1, лист 1

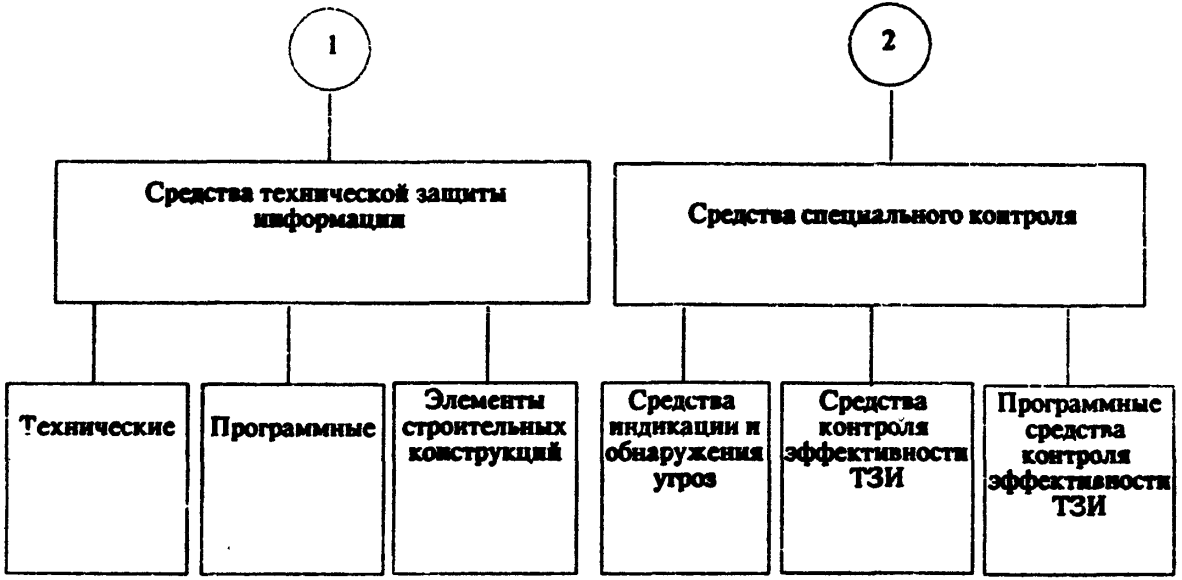

Рисунок А. 1, лист 2

УДК 006.3:002 01.140.20 Т62

Ключевые слова: информация, защита информации, техническая защита информации, средства обеспечения информационой деятельности, средства технической защиты информации, план защиты, аттестация

Редактор Г. Ярмиш
Технічний редактор О. Касіч
Коректор Т. Нагорна

Підписано до друку 26.05.97 Формат 60×84 1/16
Ум. друк. арк 1,86. Зам. 1123 Ціна договірна

Дільниця оперативного друку УкрНДІССІ
252006, Київ-6, вул Горького, 174