ДСТУ 3396.0—96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УКРАИНЫ

Защита информации

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Основные положения

Издание официальное

Киев
ГОССТАНДАРТ УКРАИНЫ
1996

ПРЕДИСЛОВИЕ

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

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Госстандарта Украины от 11 октября 1996 г. № 423

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, А. Новиченко, В. Гелевера, И. Арутюнова

СОДЕРЖАНИЕ

ДСТУ 3396.0—96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УКРАИНЫ

ЗАЩИТА ИНФОРМАЦИИ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Основные положения

ЗАХИСТ ІНФОРМАЦІЇ

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Основні положення

INFORMATION PROTECTION

TECHNICAL PROTECTION OF INFORMATION

Basic principles

Дата введения 1997—01—01

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт устанавливает объект защиты, цель, основные организационно-технические положения технической защиты информации (ТЗИ), неправомерный доступ к которой может нанести ущерб гражданам, организациям (юридическим лицам) и государству, а также категории нормативных документов по 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.

Издание официальное

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте приведены ссылки на следующие документы:

ДСТУ 1.0—93 Государственная система стандартизации Украины. Основные положения;

ДСТУ 1.2—93 Государственная система стандартизации Украины Порядок разработки государственных стандартов;

ДСТУ 1.3—93 Государственная система стандартизации Украины. Порядок разработки, построения, изложения, оформления, согласования, утверждения, обозначения и регистрации технических условий;

ДСТУ 1.4—93 Государственная система стандартизации Украины. Стандарт предприятия. Основные положения;

ДСТУ 1.5—93 Государственная система стандартизации Украины. Общие требования к построению, изложению, оформлению и содержанию стандартов;

ДБН А.1.1—1—93 Система стандартизации и нормирования в строительстве. Основные положения;

ДБН А.1.1—2—93 Система стандартизации и нормирования в строительстве. Порядок разработки, требования к построению, изложению и оформлению нормативных документов.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Объектом технической защиты является информация, которая составляет государственную или иную предусмотренную законодательством Украины тайну, конфиденциальная информация, являющаяся государственной собственностью или переданная государству во владение пользование, распоряжение (далее— информация с ограниченным доступом — ИсОД).

3.2 Объект защиты, цель и задачи ТЗИ определяют и устанавливают лица, которые владеют, пользуются, распоряжаются ИсОД в рамках прав и полномочий, предоставленных законами Украины, подзаконными актами и нормативными документами по ТЗИ.

3.3 Носителями ИсОД могут быть физические поля, сигналы, химические вещества, образующиеся в процессе информационной деятельности, производства и эксплуатации продукции различного назначения (далее— информационная деятельность).

3.4 Средой распространения носителей ИсОД могут быть линии связи, сигнализации, управления, энергетические сети, оконечное и промежуточное оборудование, инженерные коммуникации и сооружения, ог-

раждающие строительные конструкции, а также светопроницаемые элементы зданий и сооружений (проемы), воздушная, водная и другие среды, почва, растительность и т. п.

3.5 Утечка или нарушение целостности ИсОД (искажение, модификация, разрушение, уничтожение) могут произойти в результате реализации угроз безопасности информации (далее—угроза).

3.6 Целью ТЗИ является предотвращение утечки или нарушения целостности ИсОД.

3.7 Цель ТЗИ может быть достигнута построением системы защиты информации, которая представляет собой организованную совокупность методов и средств обеспечения ТЗИ.

Техническая защита информации осуществляется поэтапно:

1 этап — определение и анализ угроз;

2 этап — разработка системы защиты информации;

3 этап — реализация плана защиты информации;

4 этап — контроль фукционирования и управление системой защиты информации.

4 ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Определение и анализ угроз

4.1.1 На первом этапе необходимо осуществить анализ объектов защиты, ситуационного плана, условий функционирования предприятия, учреждения, организации, оценить вероятность проявления угроз и ожидаемый ущерб от их реализации, подготовить исходные данные для построения частной модели угроз.

4.1.2 Источниками угроз может быть деятельность иностранных разведок, а также преднамеренные или непреднамеренные действия юридических и физических лиц.

4.1.3 Угрозы могут осуществляться:

— по техническим каналам, включающим каналы побочных электромагнитных излучений и наводок, акустические, оптические, радио-, радиотехнические, химические и другие каналы;

— по каналам специального воздействия путем формирования полей и сигналов в целях разрушения системы защиты или нарушения целостности информации;

— несанкционированным доступом путем подключения к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, преодоления мер защиты для использования информации или навязыва-

ния ложной информации, применения закладных устройств и программ, внедрения компьютерных вирусов.

4.1.4 Описание угроз и схематическое представление путей их осуществления составляют частную модель угроз.

4.2 Разработка системы защиты информации

4.2.1 На втором этапе следует осуществить разработку плана ТЗИ, включающего организационные, первичные технические и основные технические меры защиты ИсОД, определить зоны безопасности информации.

Организационные меры регламентируют порядок информационной деятельности с учетом норм и требований по ТЗИ для всех периодов жизненного цикла объекта защиты.

Первичные технические меры предусматривают защиту информации блокированием угроз без использования средств ТЗИ.

Основные технические меры предусматривают защиту информации с использованием средств обеспечения ТЗИ.

4.2.2 Для технической защиты информации следует применять способ скрытия или способ технической дезинформации.

4.2.3 Меры защиты информации должны:

— быть адекватны угрозам;

— быть разработаны с учетом возможного ущерба от их реализации и стоимости защитных мер и вносимых ими ограничений;

— обеспечивать заданную эффективность защиты информации на установленном уровне в течение времени ограничения доступа к ней или возможности осуществления угроз.

4.2.4 Уровень защиты информации определяется системой количественных и качественных показателей, обеспечивающих решение задач защиты информации на основе норм и требований ТЗИ.

4.2.5 Минимально необходимый уровень защиты информации обеспечивается ограничительными и фрагментарными мерами противодействия наиболее опасной угрозе.

Повышение уровня защиты информации достигается наращиванием технических мер противодействия множеству угроз.

4.2.6 Порядок расчета и инструментального определения зон безопасности информации, реализации мер ТЗИ, расчета эффективности защиты и порядок аттестации технических средств обеспечения информационной деятельности, рабочих мест (помещений) устанавливаются нормативными документами по ТЗИ.

4.3 Реализация плана защиты информации

4.3.1 На третьем этапе следует реализовать организационные, первичные технические и основные технические меры защиты ИсОД, установить необходимые зоны безопасности информации, провести аттестацию технических средств обеспечения информационной деятельности, рабочих мест (помещений) на соответствие требованиям по безопасности информации.

4.3.2 Техническая защита информации обеспечивается применением защищенных программ и технических средств обеспечения информационной деятельности, программных и технических средств защиты информации (далее — средства ТЗИ) и средств контроля, имеющих сертификат соответствия требованиям нормативных документов по технической защите системы УкрСЕПРО или разрешение на их использование органа, уполномоченного Кабинетом Министров Украины, а также применением специальных инженерно-технических сооружений, средств и систем (далее— средства обеспечения ТЗИ).

4.3.3 Средства ТЗИ могут функционировать автономно или совместно с техническими средствами обеспечения информационной деятельности в виде самостоятельных устройств или встроенных в них составных элементов.

4.3.4 Состав средств обеспечения ТЗИ, перечень их поставщиков, а также услуг по установке, монтажу, наладке и обслуживанию определяются лицами, которые владеют, пользуются и распоряжаются ИсОД самостоятельно или по рекомендациям специалистов по ТЗИ в соответствии с нормативными документами по ТЗИ.

4.3.5 Предоставление услуг по ТЗИ, аттестацию и сервисное обслуживание средств обеспечения ТЗИ могут осуществлять юридические и физические лица, имеющие лицензию на право проведения этих работ, выданную органом, уполномоченным Кабинетом Министров Украины.

4.4 Контроль функционирования и управление системой защиты информации

4.4.1 На четвертом этапе следует провести анализ функционирования системы защиты информации, проверку выполнения мер ТЗИ, контроль эффективности защиты, подготовить и выдать исходные данные для управления системой защиты информации.

4.4.2 Управление системой защиты информации заключается в адаптации мер ТЗИ к текущей задаче защиты информации.

По фактам изменения условий осуществления или выявления новых угроз меры ТЗИ реализуются в кратчайший срок.

4.4.3 В случае необходимости повышения уровня защиты информации необходимо выполнить работы, предусмотренные 1, 2 и 3 этапами построения системы защиты информации.

4.4.4 Порядок проведения проверок и контроля эффективности защиты информации устанавливается нормативными документами по ТЗИ.

5 НОРМАТИВНЫЕ ДОКУМЕНТЫ ПО ТЗИ

5.1 Нормативные документы разрабатываются в ходе проведения комплекса работ по стандартизации и нормированию в области ТЗИ.

5.2 Нормативные документы должны обеспечивать:

— проведение единой технической политики;

— создание и развитие единой терминологической системы;

— функционирование многоуровневых систем защиты информации на основе взаимоувязанных положений, правил, методик, требований и норм;

— функционирование систем сертификации, лицензирования и аттестации согласно требованиям безопасности информации;

— развитие сферы услуг в области ТЗИ;

— установление порядка разработки, производства, эксплуатации средств обеспечения ТЗИ;

— организацию проектирования строительных работ в части обеспечения ТЗИ;

— подготовку и переподготовку кадров в системе ТЗИ.

5.3 Нормативные документы по ТЗИ подразделяются на:

— нормативные документы по стандартизации в области ТЗИ;

— государственные стандарты или приравненные к ним нормативные документы;

— нормативные акты межведомственного значения, регистрируемые в Министерстве юстиции Украины;

— нормативные документы межведомственного значения технического характера, регистрируемые органом, уполномоченным Кабинетом Министров Украины;

— нормативные документы ведомственного значения органов государственной власти и органов местного самоуправления.

5.4 Порядок проведения работ по стандартизации и нормированию в области ТЗИ устанавливается ДСТУ 1.0, ДБН А.1.1—1, документами системы ТЗИ.

5.5 Порядок разработки, оформления, согласования, утверждения, регистрации, издания, внедрения, проверки, пересмотра, изменения и отмены нормативных документов устанавливается ДСТУ 1.2, ДСТУ 1.3, ДСТУ 1.4, ДСТУ 1.5, ДБН А. 1.1—2, документами системы ТЗИ.

УДК 006.3:002 35.020 Т62

Ключевые слова: информация, техническая защита информации, система защиты информации, план защиты информации, нормативный документ

Редактор Т. Голованова
Технічний редактор О. Касіч

Підписано до друку 23.12.96. Формат 60×84 1/16.
Ум. друк. арк. 1,39. Зам. 6 Ціна договірна.

Дільниця оперативного друку Укр НДІССІ
252006 Київ-6, вул. Горького, 174