ДСТУ 3396.0-96

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

Захист інформації

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Основні положення

Видання офіційне

Київ
ДЕРЖСТАНДАРТ УКРАЇНИ
1996

ПЕРЕДМОВА

1 РОЗРОБЛЕНО І ВНЕСЕНО Державною службою України з питань технічного захисту інформації

2 ЗАТВЕРДЖЕНО \ ВВЕДЕНО В ДІЮ наказом Держстандарту України від 11 жовтня І996 р. № 423

3 У цьому стандарті реалізовано норми законів України «Про інформацію», «Про державну таємницю», «Про захист інформації в автоматизованих системах»

4 ВВЕДЕНО ВПЕРШЕ

5 РОЗРОБНИКИ: О. Баранов, А. Новіченко, Б. Гелевера, 1. Арутюнова

ЗМІСТ

ДСГУ 3396.0-96

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

ЗАХИСТ ІНФОРМАЦІЇ

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Основні положення

ЗАШИТА ИНФОРМАЦИИ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Основные положения

Чинний від 1997—01—01

1 ГАЛУЗЬ ВИКОРИСТАННЯ

Цей стандарт установлює об'єкт захисту, мету, основні організаційно-технічні положення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів зТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян — суб'єктів підприємницькоїдіяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

Видання офіційне

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті наведено посилання на такі документи:

ДСТУ 1.0—93 Державна система стандартизації України. Основні положення;

ДСТУ 1.2—93 Державна система стандартизації України. Порядок розроблення державних стандартів;

ДСТУ 1.3—93 Державна система стандартизації України. Порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов;

ДСТУ 1.4—93 Державна система стандартизації України. Стандарт підприємства. Основні положення;

ДСТУ 1.5—93 Державна система стандартизації України. Загальні вимоги до побудови, викладу, оформлення і змісту стандартів;

ДБН А. 1.1 — і—93 Система стандартизації та нормування в будівництві. Основні положення;

ДБН А.1.1—2—93 Система стандартизації та нормування в будівництві. Порядок розробки, вимоги до побудови, викладу та оформлення нормативних документів.

3 ЗАГАЛЬНІ ПОЛОЖЕННЯ

3.1 Об'єктом технічного захисту с інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження (далі— інформація з обмеженим доступом — ІзОД).

3.2 Об'єкт захисту, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами з ТЗІ.

3.3 Носіями ІзОД можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення (далі— інформаційна діяльність).

3.4 Середовищем поширення носіїв ІзОД можуть бути лінії зв'язку, сигналізації, керування, енергетичні мережі, прикінцевеі проміжне обладнання, інженерні комунікації і споруди, відгороджувалі ні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інше середовища, грунт, рослинність тощо.

3.5 Витік або порушення цілісності ІзОД (спотворення, модифікація, руйнування, знищення) можуть бути результатом реалізації загроз безпеці інформації (далі—загроза).

3.6 Метою ТЗІ с запобігання витоку або порушенню цілісності ІзОД.

3.7 Мста ТЗІ може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ.

Технічний захист інформації здійснюється поетапно:

1 етап — визначення й аналіз загроз;

2 етап — розроблення системи захисту інформації;

3 етап — реалізація плану захисту інформації;

4 етап — контроль фукціювання та керування системою захисту інформації.

4 ПОБУДОВА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Визначення й аналіз загроз

4.1.1 На першому етапі необхідно здійснити аналіз об'єктів захисту, ситуаційного плану, умов функціюпання підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду під їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.

4.1.2 Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

4.1.3 Загрози можуть здійснюватися:

— технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

— каналами спеціального впливу шляхом формування полів і сигналів з мстою руйнування системи захисту або порушення цілісності інформації; .

— несанкційованнм доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зарсстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування підкладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

4.1.4 Опис загроз і схематичне подання шляхів їх здійснення складають окрему модель загроз.

4.2 Розроблення системи захисту інформації

4 2.1 На другому етапі слід здійснити розроблення плану ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначити зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життевого циклу об'єкта захисту.

Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

4.2.2 Для технічного захисту інформації слід застосовувати спосіб приховування або спосіб технічної дезінформації.

4.2.3 Заходи захисту інформації повинні:

— бути відповідними загрозам;

— бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;

— забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

4.2.4 Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв'язання завдання захисту інформації на основі норм та вимог ТЗІ.

4.2.5 Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

4.2.6 Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами з ТЗІ

4.3 Реалізація плану захисту інформації

4.3.1 На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні он» Безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщені.) на відповідність вимогам безпеки інформації.

4.3.2 Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (далі — засоби ТЗІ) та засобів контролю, які мають сертифікат відповідності вимогам нормативних документів з технічного захисту системи УкрСЕПРО або дозпіл на їх використання від органу, уповноваженого Кабінетом Міністрів України, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем (далі— засоби забезпечення ТЗІ).

4.3.3 Засоби ТЗІ можуть функціюватн автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

4.3.4 Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, які володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами з ТЗІ.

4.3.5 Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні скоби, які мають ліцензію на право проведення цих робіт, видану органом, уповноваженим Кабінетом Міністрів України.

4.4 Контроль функціювання та керування системою захисту інформації

4.4.1 На четвертому етапі слід провести аналіз функціювання системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати засадничі дані для керування системою захисту інформації.

4.4.2 Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації.

За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

4.4.3 У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені 1, 2 та 3 етапами побудови системи захисту інформації.

4.4.4 Порядок проведення перевірок і контролю ефективності захисту інформації встановлюється нормативними документами з ТЗІ.

5 НОРМАТИВНІ ДОКУМЕНТИ З ТЗІ

5.1 Нормативні документи розробляються в ході проведення комплексу робіт із стандартизації та нормування у галузі ТЗІ. .

5.2 Нормативні документи повинні забезпечувати:

— проведення єдиної технічної політики;

— створення і розвиток сдиної термінологічної системи;

— функціювання багаторівневих систем захисту інформації на основі взаемнопогодженнх положень, правил/методик, вимог та норм;

— функціювання систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації;

— розвиток сфери послуг у галузі ТЗІ;

— установлення порядку розроблення, виробництва, експлуатації засобів забезпечення ТЗІ;

— організацію проектування будівельних робіт у частині забезпечення ТЗІ;

— підготовку та перепідготовку кадрів у системі ТЗІ.

5.3 Нормативні документи з ТЗІ поділяються на:

— нормативні документи із стандартизації у галузі ТЗІ;

— державні стандарти та прирівняні до них нормативні документи;

— нормативні акти міжвідомчого значення, шо реєструються у Міністерстві юстиції України;

— нормативні документи міжвідомчого значення технічного характеру, то реєструються органом, уповноваженим Кабінетом Міністрів України;

— нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

5.4 Порядок проведення робіт із стандартизації та нормування у галузі ТЗІ встановлюється ДСТУ І 0, ДОН А.І.І—І, документами системи ТЗІ.

5.5 Порядок розроблення, оформлення, погодження, затвердження, реєстрації, видання, впровадження, перевірки, перегляду, зміни та скасування нормативних документів установлюється ДСТУ 1.2, ДСТУ І.З, ДСТУ 1.4, ДСТУ 1.5.ДБН А. 1.1-2, документами системи ТЗІ.

УДК 006.3:002 35.020 Т62

Ключові слова: інформація, технічний захист інформації, система захисту інформації, план захисту інформації, нормативний документ

*

I

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

С.

ДСТУ 3396.0-96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УКРАИНЫ

ЗАЩИТА ИНФОРМАЦИИ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Основные положения

ЗАХИСТ ІНФОРМАЦІЇ

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Основні положення

Дата введения 1997—0)—01

I 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 псех 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 н 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, распоряжс ние (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,

ограждающие 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 ожи даемый ущерб этих 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 их учений 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 зарегистрироанного пользователя, преодоления мер защиты для использования информации или навязыва-

нии 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 зашиты информации определяется системой количественных и качественные показателей, обеспечивающих решение задачи 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 сооружении, 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.

Пофактам 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 осгроенкя системы защиты информации.

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

5 НОРМАТИВНЫЕ ДОКУМЕНТЫ ПО ТЗИ

5.1 Нормативные документы разрабатываются в ходе проведения омплекса 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 а 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 обестеченияТЗИ

— 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 АЛЛ—1, документами системы ТЗИ.

5.5 Порядок разработки, оформления, согласовании, 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.