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 рядка 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

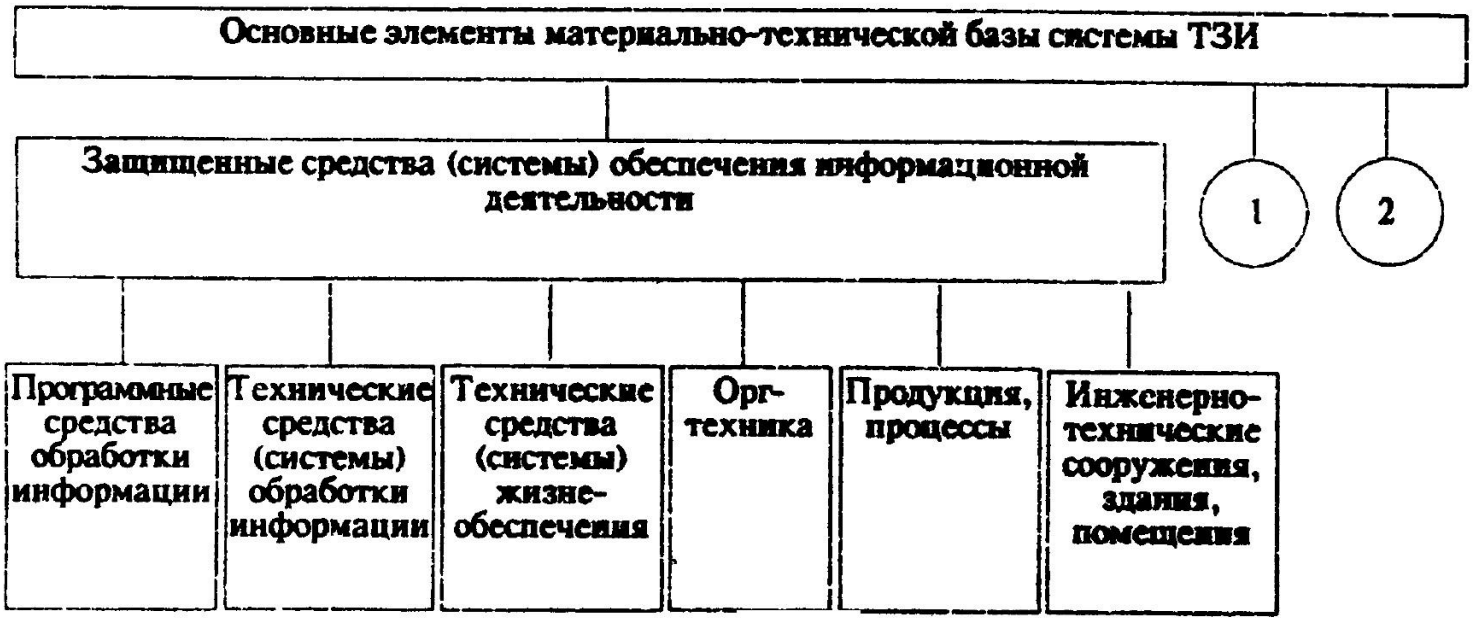

Рисунок А. 1, лист 1

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

ДСТУ 3396.1—96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УКРАИНЫ

Защита информации

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Порядок проведения работ

Издание официальное

Киев
ГОССТАНДАРТ УКРАИНЫ
1997

ПЕРЕДМОВА

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

2 ЗАТВЕРДЖЕНО І ВВЕДЕНО ВДІЮ наказом Держстандарту України від 19 грудня 1996 р. №51

3 В цьому стандарті реалізовані норми Закону України «Про інформацію», «Про державну таємницю», «Про захист інформації в автоматизованих системах»

4 ВВЕДЕНО ВПЕРШЕ

5 РОЗРОБНИКИ: А. Баранов, канд. Техн. Наук, В. Дюпін, А. Новиченко, В. Гелевера, І. Арутюнова

ЗМІСТ

ДСТУ 3396.1—96

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

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

Чинний від 01.07.1997 р.

1 ГАЛУЗЬ ВИКОРИСТАННЯ

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації (ТЗІ).

Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян - суб`єктів підприємницької діяльності, 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.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті наведено посилання на такий стандарт:

ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

Видання офіційне

3 ЗАГАЛЬНІ ПОЛОЖЕННЯ

3.1 Інформація з обмеженим доступом (ІзОД) в процесі інформаційної діяльності (ІД), основними видами якої є одержання, використання, поширення та зберігання ІзОД, може зазнавати впливу загроз її безпеці (далі - загроза), у результаті чого може відбутися її витік або порушення цілісності інформації.

Схильність ІзОД до впливу загроз визначає її вразливість.

Здатність системи захисту інформації протистояти впливу загроз визначає захищеність ІзОД.

3.2 Можливі такі варіанти захисту інформації:

- досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів ІД;
- досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД;
- досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД.

Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту.

Захист інформації, яка становить державну таємницю, забезпечується, як правило, застосуванням третього варіанту.

3.3 Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації повинні відповідати зазначеним в ДСТУ 3396.0-96 етапам функціонування системи захисту інформації і полягає в:

- проведенні обстеження підприємства, установи, організації (далі - підприємство);
- розробленні і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ (додаток А);
- прийманні робіт з ТЗІ;
- атестації засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ.

3.4 Порядок проведення робіт з ТЗІ або окремих їхніх етапів установлюється наказом (розпорядженням) керівника підприємства.

Роботи повинні виконуватися силами підприємства під керівництвом спеціалістів з ТЗІ.

Для участі в роботах, подання методичної допомоги, оцінювання повноти та якості реалізації заходів захисту можуть залучатися спеціалісти з ТЗІ інших організацій, які мають ліцензію органа, уповноваженого Кабінетом Міністрів України.

4 ОРГАНІЗАЦІЯ ПРОВЕДЕННЯ ОБСТЕЖЕННЯ

4.1 Метою обстеження підприємства є вивчення його ІД, визначення об`єктів захисту - ІзОД, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.

4.2 Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника підприємства.

4.3 У ході обстеження необхідно:

- провести аналіз умов функціонування підприємства, його розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;
- дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;
- вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, уземлення, автоматизації, пожежної та охоронної сигналізацій), а також інженерних комунікацій та металоконструкцій;
- дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі - оброблення) інформації і провести необхідні вимірювання;
- визначити наявність та технічний стан засобів забезпечення ТЗІ;
- перевірити наявність на підприємстві нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;
- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;
- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;
- визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

4.4 За результатами обстеження слід скласти акт, який повинен бути затверджений керівником підприємства.

4.5 Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна включати:

- генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;
- схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД;
- оцінку шкоди, яка передбачається від реалізації загроз.

5 ОРГАНІЗАЦІЯ РОЗРОБЛЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

5.1 На підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання (ТЗ) на розроблення системи захисту інформації.

5.2 ТЗ повинно включати основні розділи:

- вимоги до системи захисту інформації;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;
- порядок внесення змін і доповнень до розділів ТЗ;
- вимоги до порядку проведення випробування системи захисту.

5.3 Основою функціонування системи захисту інформації є план ТЗІ, що повинен містити такі документи:

- перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування;
- інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;
- інструкції, що встановлюють обов`язки, права та відповідальність персоналу;
- календарний план ТЗІ.

5.4 ТЗ і план ТЗІ розробляють спеціалісти з ТЗІ, узгоджують із зацікавленими підрозділами (організаціями).

Затверджує їх керівник підприємства.

6 РЕАЛІЗАЦІЯ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЗАХИСТУ

6.1 Організаційні заходи захисту інформації - комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

6.2 У процесі розроблення і реалізації організаційних заходів потрібно:

- визначити окремі задачі захисту ІзОД;
- обгрунтувати структуру і технологію функціонування системи захисту інформації;
- розробити і впровадити правила реалізації заходів ТЗІ;
- визначити і встановити права та обов`язки підрозділів та осіб, що беруть участь в обробленні ІзОД;
- придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними підприємство;
- установити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;
- установити порядок контролю функціонування системи захисту інформації та її якісних характеристик;
- визначити зони безпеки інформації;
- установити порядок проведення атестації системи захисту інформації, її елементів і розробити програми атестаційного випробування;
- забезпечити керування системою захисту інформації.

6.3 Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно:

- вивчати й аналізувати технологію проходження ІзОД у процесі ІД;
- оцінювати схильність ІзОД до впливу загроз у конкретний момент часу;
- оцінювати очікувану ефективність застосування засобів забезпечення ТЗІ;
- визначати (за необхідності) додаткову потребу в засобах забезпечення ТЗІ;
- здійснювати збирання, оброблення та реєстрацію даних, які відносяться до ТЗІ;
- розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

7 РЕАЛІЗАЦІЯ ПЕРВИННИХ ТЕХНІЧНИХ ЗАХОДІВ ЗАХИСТУ

7.1 У процесі реалізації первинних технічних заходів потрібно забезпечити:

- блокування каналів витоку інформації;
- блокування несанкціонованого доступу до інформації чи її носіїв;
- перевірку справності та працездатності технічних засобів забезпечення ІД.

7.2 Блокування каналів витоку інформації може здійснюватися:

- демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано з життєзабезпеченням підприємства та обробленням ІзОД;
- видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів, з приміщень, де циркулює ІзОД;
- тимчасовим відключенням технічних засобів, які не беруть участі в обробленні ІзОД, від ліній зв'язку, сигналізації, керування та енергетичних мереж;
- застосуванням способів та схемних рішень із захисту інформації, що не порушують основних технічних характеристик засобів забезпечення ІД.

7.3 Блокування несанкціонованого доступу до інформації або її носіїв може здійснюватися:

- створенням умов роботи в межах установленого регламенту;
- унеможливленням використання програмних, програмно-апаратних засобів, що не пройшли перевірки (випробування).

7.4 Перевірку справності та працездатності технічних засобів і систем забезпечення ІД необхідно проводити відповідно до експлуатаційних документів.

Виявлені несправні блоки й елементи можуть сприяти витоку або порушенню цілісності інформації і підлягають негайній заміні (демонтуванню).

8 РЕАЛІЗАЦІЯ ОСНОВНИХ ТЕХНІЧНИХ ЗАХОДІВ ЗАХИСТУ

8.1 У процесі реалізації основних технічних заходів захисту потрібно:

- установити засоби виявлення та індикації загроз і перевірити їхню працездатність;
- установити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність;
- застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє функціональне тестування і тестування на відповідність вимогам захищеності;
- застосувати спеціальні інженерно-технічні споруди, засоби (системи).

8.2 Вибір засобів забезпечення ТЗІ зумовлюється фрагментарним або комплексним способом захисту інформації.

Фрагментарний захист забезпечує протидію певній загрозі.

Комплексний захист забезпечує одночасну протидію безлічі загроз.

8.3 Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) ІзОД про витік інформації чи порушення її цілісності.

8.4 Засоби ТЗІ застосовуються автономно або спільно з технічними засобами забезпечення ІД для пасивного або активного приховування ІзОД.

Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани.

Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

8.5 Програмні засоби застосовуються для забезпечення:

- ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації;
- розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем;
- цілісності інформації та конфігурації автоматизованих систем;
- реєстрації та обліку дій користувачів;
- маскування оброблюваної інформації;
- реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій.

8.6 Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації.

До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо.

8.7 Розміщення, монтування та прокладання спеціальних інженерно-технічних засобів і систем, серед них систем уземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог нормативних документів з ТЗІ.

8.8 Технічні характеристики, порядок застосування та перевірки засобів забезпечення ТЗІ наводять у відповідній експлуатаційній документації.

9 ПРИЙМАННЯ, ВИЗНАЧЕННЯ ПОВНОТИ ТА ЯКОСТІ РОБІТ

9.1 За результатами виконання рекомендацій акта обстеження та реалізації заходів захисту ІзОД слід скласти у довільній формі акт приймання робіт з ТЗІ, який повинен підписати виконавець робіт, особа, відповідальна за ТЗІ, та затвердити керівник підприємства.

Примітка. За потреби акт приймання робіт може бути погоджений із зацікавленими організаціями.

9.2 Для визначення повноти та якості робіт з ТЗІ слід провести атестацію. Атестація виконується організаціями, які мають ліцензії на право діяльності в галузі ТЗІ.

9.3 Об`єктами атестації є системи забезпечення ІД та їхні окремі елементи, де циркулює інформація, що підлягає технічному захисту.

9.4 У ході атестації потрібно:

- установити відповідність об`єкта, що атестується, вимогам ТЗІ;
- оцінити якість та надійність заходів захисту інформації;
- оцінити повноту та достатність технічної документації для об`єкта атестації;
- визначити необхідність внесення змін і доповнень до організаційно-розпорядчих документів тощо.

Порядок атестації встановлюється нормативними документами системи ТЗІ.

Додаток А
(довідковий)
Склад засобів забезпечення технічного захисту інформації

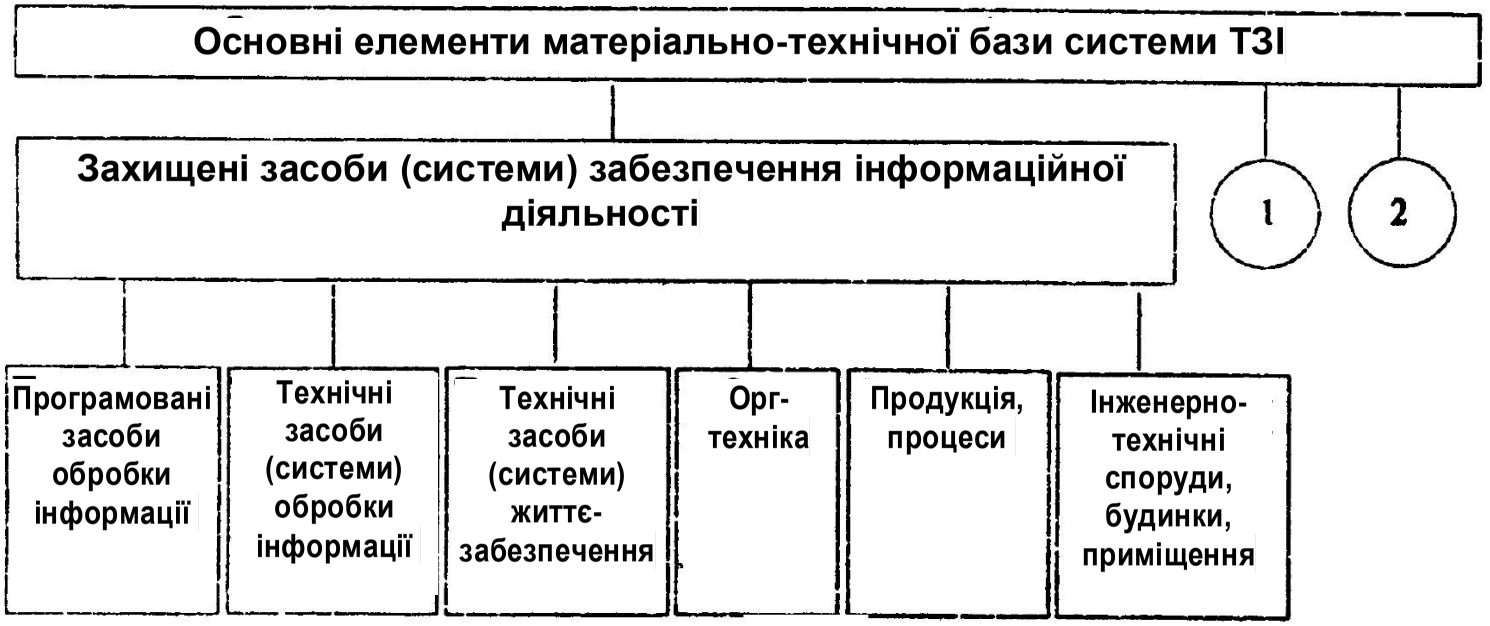

Рисунок А.1, аркуш 1

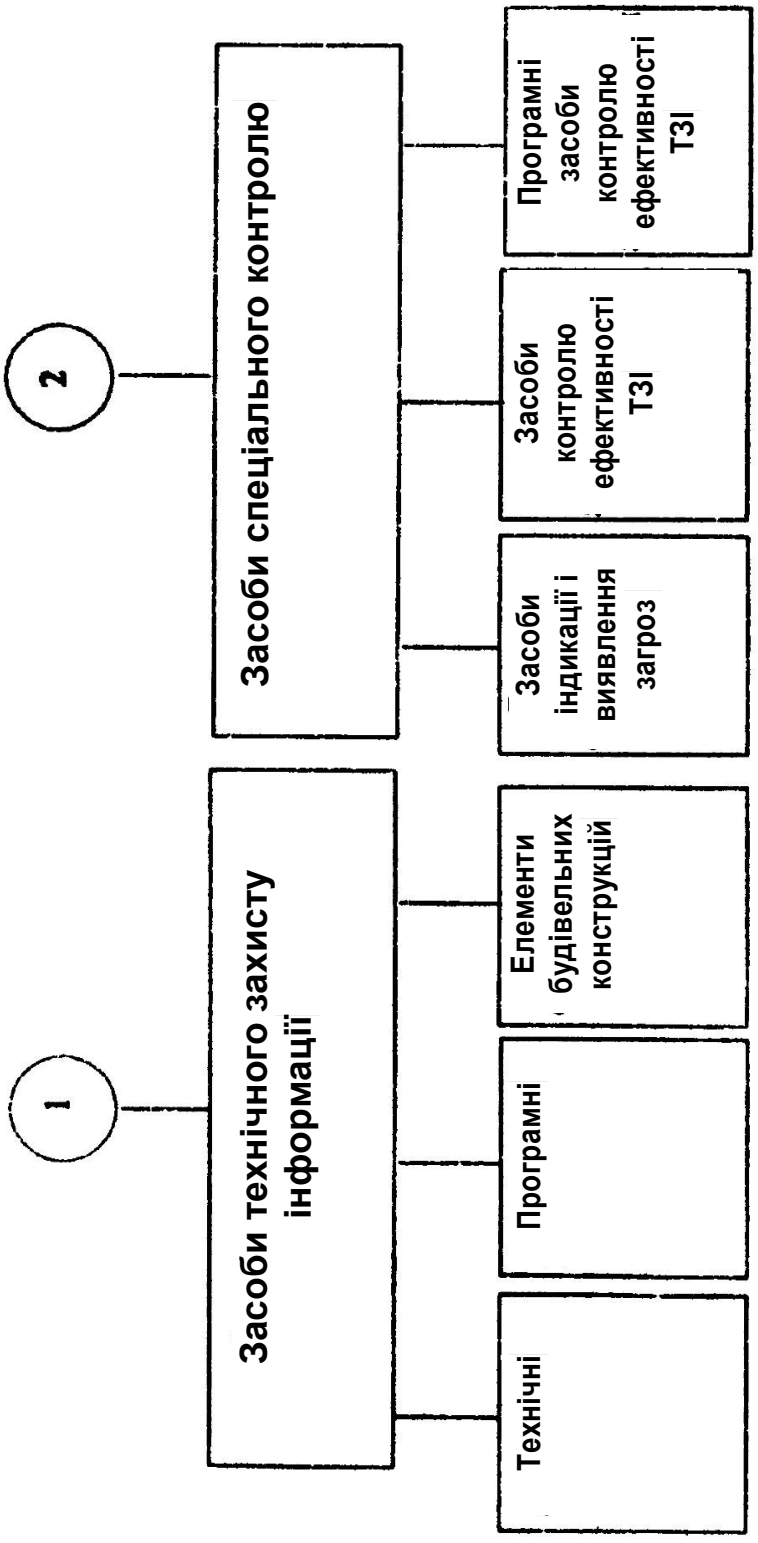

Рисунок А.1, аркуш 2

УДК 006.3:002 01.120.20 Т62

Ключові слова: інформація, захист інформації, технічний захист інформації, засоби забезпечення інформаційної діяльності, засоби технічного захисту інформації, план захисту, атестація

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 УркНДІССІ
252006 Київ-6, вул. Горького, 174