ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

Захист інформації

Технічний захист інформації.
Порядок проведення робіт

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.

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 функціювання 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 функціювання 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 функціювання 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 обгрунтовано 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 несанкційованого 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 функціювання 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 функціювання 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 функціювання 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 функціювання системи захисту інформації та її якісних характеристик;
- визначити зони безпеки інформації;
- установити порядок проведення атестації системи захисту інформаціїі, 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 несанкційованого 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 несанкційованого 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 функційне 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 несанкційованих 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.