ДСТУ 3396.0-96

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

Захист інформації
Технічний захист інформації
Основні положення

Защита информации
Техническая защита информации
Основные положения

Information protection
Technical protection of information
Basic principles

Чинний від 01.01.1997 р.

1 Галузь використання

Цей стандарт установлює об’єкт, мету, основні організаційнотехнічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Вимоги стандарту обов’язкові для підприємств та установ усіх форм власності і 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 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.1.1-1-93 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 є 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, 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 системи 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, прикінцеве і проміжне обладнання, інженерні комунікації і споруди, відгороджувальні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інші 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 є запобігання витоку або порушенню цілісності ІзОД.

3.7 Мета 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 функціювання 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 ТЗІ, ситуаційного плану, умов функціювання підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду від 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 метою руйнування системи захисту або порушення цілісності інформації;
- несанкційованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних 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 життєвого циклу об’єкта ТЗІ.

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 реа-лізації 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 системи 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 зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) 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 контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Мі-ністрів України органу, а також застосуванням спеціальних інженернотехнічних споруд, засобів і систем (далі - засоби забезпечення ТЗІ).

4.3.3 Засоби ТЗІ можуть функціювати 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, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ.

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

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.

5 Нормативні документи системи 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 єдиної термінологічної системи;
- функціювання багаторівневих систем захисту інформації на основі взаємнопогоджених 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, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апа-ратури;
- організацію проектування будівельних робіт у частині забезпечення ТЗІ;
- підготовку та перепідготовку кадрів у системі ТЗІ.

5.3 Нормативні документи системи ТЗІ поділяються на:

- нормативні документи із стандартизації у галузі ТЗІ;
- державні стандарти та прирівняні до них нормативні документи;

- нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України;

- нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів органом;

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

5.4 Порядок проведення робіт із стандартизації та нормування в галузі ТЗІ встановлюється ДСТУ 1.0, ДБН А.1.1-1, документами системи ТЗІ.

5.5 Порядок розроблення, оформлення, узгодження, затвердження, реєстрації, видання, впровадження, перевірки, перегляду, зміни та скасування нормативних документів установлюється ДСТУ 1.2, ДСТУ 1.3, ДСТУ 1.4, ДСТУ 1.5, ДБН А.1.1-2, документами системи ТЗІ.