УДК 316.776:351.741:34:650.0128

Попов Анатолій, ст. 3 курсу Фізико-технічного інституту; науковий керівник – ст. викл. Василенко О. Д. (Національний технічний університет України «Київський політехнічний інститут», м. Київ)

ОЦІНКА ЯКОСТІ РОБІТ ТА ПОСЛУГ У ГАЛУЗІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. *В статті досліджено нормативні документи, що регламентують функціонування системи технічного захисту інформації. Розкрито порядок виконання робіт зі створення комплексних систем захисту інформації та одержання атестату відповідності, порядок атестування системи технічного захисту інформації, правила проведення робіт із сертифікації засобів захисту інформації, організацію проведення перевірок стану ТЗІ..*
Ключові слова: *технічний захист інформації (ТЗІ), системи технічного захисту інформації.*

Аннотация. *В статье исследованы нормативные документы, регламентирующие функционирование системы технической защиты информации. Раскрыты порядок выполнения работ по созданию комплексных систем защиты информации и получения аттестата соответствия, порядок аттестации системы технической защиты информации, правила проведения работ по сертификации средств защиты информации, организация проведения проверок состояния ТЗИ.*
Ключевые слова: *техническая защита информации (ТЗИ), системы технической защиты информации.*

Annotation*. The article analyzes the regulatory documents governing the functioning of the technical information protection system. The aim of work execution is to establish information protection complex systems and obtaining a certificate of compliance. Procedure for information security certification, organization of inspections of technical information protection are determined. The general description of the methodology of functional safety services assessment is carried out.*
Keywords: *technical information protection, technical information protection system.*

Функціонування системи технічного захисту інформації здійснюється з урахуванням необхідності гарантування відповідності рівня захищеності інформації вимогам нормативних документів. При цьому належну якість

робіт із технічного захисту інформації можна забезпечити за умови залучення висококваліфікованих спеціалістів, які мають відповідну фахову підготовку й досвід роботи, та за відповідного технічного оснащення. З урахуванням зазначеного, всі суб'єкти системи технічного захисту інформації, які здійснюють свою діяльність у сфері технічного захисту інформації, мають проходити відповідну атестацію: суб'єкти господарської діяльності отримують ліцензію відповідно до Закону України «Про ліцензування певних видів господарської діяльності». Наразі в Україні здійснюють діяльність близько 230 ліцензіатів у сфері технічного захисту інформації, а державні органи мають дозволи на право виконання робіт з технічного захисту інформації для власних потреб.

Окремі питання технічного захисту інформації досліджували такі українські й російські вчені: С. Байдак, С. Васильчак, В. Герасименко, В. Домарьов, А. Ісаєв, А. Малюк, О. Фролов, В. Хорошко, А. Чекатков, В. Ярочкін та ін.

Метою нашої статті є дослідження нормативних документів що регламентують функціонування системи технічного захисту інформації; порядок виконання робіт зі створення КСЗІ (комплексні системи захисту інформації) та одержання Атестату відповідності; порядок атестування системи технічного захисту інформації; правила проведення робіт із сертифікації засобів захисту інформації; організацію проведення перевірок стану ТЗІ; загальний опис методології проведення оцінювання функціональних послуг безпеки.

Основи організації та порядок захисту державних інформаційних ресурсів в мережаж передачі даних (МПД) загального користування або подвійного призначення визначені нормативно-правовим актом «Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах», затвердженим наказом ДСТСЗІ СБ України від 24.12.2001 р. №76 і зареєстрованим у Міністерстві юстиції України 11.01.2002 р. за №27/6315 (далі – Порядок) [1].

Відповідно до п.п. 12–20 Порядку оператори МПД повинні забезпечити створення, упровадження та супроводження на кожному з вузлів комутації МПД комплексної системи захисту інформації, яка є сукупністю технічних, криптографічних, організаційних та інших заходів і засобів захисту, спрямованих на недопущення блокування та/або модифікації інформації під час її передавання [1].

В мережах загального користування або подвійного призначення повинна виключатися можливість несанкціонованого копіювання та зберігання інформації користувачів. КСЗІ повинна забезпечувати цілісність інформації, що передається мережею, шляхом забезпечення доступу до неї тільки персоналу МПД у відповідності з встановленими функціональними повноваженнями. КСЗІ МПД веде облік і здійснює

реєстрацію подій, які пов'язані із безпосереднім доступом (спробами доступу) до інформації, здійснює періодичний контроль за такими подіями та забезпечує захист реєстраційної інформації від несанкціонованої модифікації, руйнування або знищення [2].

Послуги МПД надаються тільки зареєстрованим користувачам за умови їх достовірного розпізнавання. Обов'язковою умовою є можливість однозначного встановлення належності інформації, що передається МПД, певному користувачеві; встановлення факту передавання або одержання оператором чи користувачем певної інформації, унеможливлення з боку користувачів несанкціонованого або неконтрольованого використання ресурсів МПД [3].

Згідно з вимогами законодавства для створення КСЗІ треба застосовувати засоби захисту, які мають сертифікати або експертні висновки щодо їх відповідності вимогам нормативних документів з ТЗІ [4].

Передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності КСЗІ вимогам захисту інформації, який надається за результатами державної експертизи в сфері технічного захисту інформації. Для одержання зазначеного атестату оператору МПД необхідно подати до ДСТСЗІ СБ України заяву про проведення державної експертизи. Порядок проведення державної експертизи, форма заяви та комплектність і зміст документів, що додаються до неї, визначено Положенням про державну експертизу в сфері технічного захисту інформації [4].

У ході атестації системи технічного захисту інформації необхідно: проаналізувати умови функціонування об'єктів інформаційної діяльності, їх розташування на місцевості (ситуаційний план) для визначення можливих джерел загроз; дослідити засоби забезпечення об'єктів інформаційної діяльності, радіус дії яких виходить за межі контрольованої території; передбачити вивчення схем засобів і систем життєзабезпечення об'єктів інформаційної діяльності (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій; дослідити інформаційні потоки, технологічні процеси передавання, одержання, використання, розповсюдження і зберігання інформації; визначити наявність та технічний стан засобів забезпечення технічного захисту інформації; перевірити наявність на об'єктах інформаційної діяльності нормативних документів, які забезпечують функціонування системи захисту інформації, а також нормативної та експлуатаційної документації, яка забезпечує інформаційну діяльність; виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у канали) кабелів і провідників; визначити технічні засоби і системи, застосування яких не обґрунтовано службовою необхідністю і які підлягають демонтуванню; визначити технічні засоби, які потребують

переобладнання (перемонтування) та встановлення засобів технічного захисту інформації [2].

Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна охоплювати: генеральний та ситуаційний плани, схеми розташування засобів і систем забезпечення інформаційної діяльності, а також інженерних комунікацій, які виходять за межі контрольованої території; схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до інформації з обмеженим доступом; оцінювання збитків, які передбачаються від реалізації можливих загроз [5].

Атестування комплексу технічного захисту інформації здійснюється за відповідними програмою і методиками випробувань. Атестування може бути первинним, поточним та позачерговим [2].

Суб'єктами атестування можуть бути: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України; організації-замовники атестування; організації-виконавці атестування [6]. Загальне керівництво сертифікаційною діяльністю у сфері захисту інформації, організація і координація робіт із сертифікації здійснюються національним органом із сертифікації – Державним комітетом України з питань технічного регулювання та споживчої політики та Державною службою спеціального зв'язку та захисту інформації України [7].

Порядок проведення робіт із сертифікації засобів захисту інформації в загальному випадку передбачає: подання заявки на сертифікацію; розгляд та прийняття рішення за заявкою із зазначенням схеми (моделі) сертифікації; обстеження чи атестацію виробництва засобів захисту інформації, що сертифікуються, або сертифікацію (оцінку) системи якості, якщо це передбачено схемою сертифікації; відбір зразків засобів захисту інформації для випробувань; ідентифікацію засобів захисту інформації; приймання випробувальними лабораторіями зразків засобів захисту інформації; випробування зразків засобів захисту інформації; аналіз одержаних результатів випробувань і прийняття рішення про можливість видачі сертифіката відповідності; видачу сертифіката відповідності, укладання ліцензійної угоди та занесення сертифікованих засобів захисту інформації до Реєстру Системи; технічний нагляд за сертифікованими засобами захисту інформації під час їх виробництва; інформування про результати робіт із сертифікації засобів захисту інформації [7].

У процесі проведення оцінювання, окрім сукупності показників, що характеризують конкретну ІТС або засіб захисту, необхідними також є: критерії оцінки, під якими слід розуміти сукупність вимог (шкала оцінки), яка використовується для оцінювання ефективності функцій захисту інформації та коректності їх реалізації; система оцінювання, під якою слід розуміти адміністративно-правову структуру, в рамках якої у певному

співтоваристві органи, що здійснюють оцінювання, застосовують критерії оцінки; методологія оцінювання, яка визначає послідовність (алгоритм) дій, що виконуються експертами при оцінюванні ефективності функцій захисту інформації та коректності їх реалізації, а також форму подання результатів.

В Україні як критерії оцінки використовуються критерії, встановлені НД ТЗІ 2.5-004-99, а також вимоги діючих НД ТЗІ щодо забезпечення захисту інформації в ІТС різного призначення. Вони надають: порівняльну шкалу для оцінювання ефективності функцій і механізмів захисту інформації від НСД, реалізованих в ІТС, а також коректності їх реалізації; базу (орієнтири) для розроблення засобів захисту інформації, оброблюваної в ІТС, від НСД [8].

Методологія оцінювання функцій захисту (функціональних послуг безпеки) передбачає виконання таких етапів робіт: попередній аналіз оцінюваного ОЕ; розроблення програми випробувань функціональних послуг безпеки; розроблення методики випробувань функціональних послуг безпеки; проведення випробувань; аналіз, документування та затвердження результатів випробувань [3].

Таким чином, обов'язковою умовою забезпечення захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, є отримання об'єктивної оцінки рівня захищеності інформації, що здійснюється шляхом проведення державної експертизи та атестації.

В процесі роботи щодо аналізу методів оцінки якості послуг та робіт у галузі технічного захисту інформації було з'ясовано, що чинні в Україні нормативно-правові акти та нормативні документи недостатньо сприяють вирішенню проблем захисту інформації загалом та технічного захисту зокрема. Має місце проблема захисту персональних даних фізичних осіб та захисту відкритої інформації, спрямованого на реалізацію законних прав та інтересів особи, суспільства та держави. Запроваджені останніми роками закони України щодо захисту інформації в інформаційно-телекомунікаційних системах, ліцензування, державного контролю господарської діяльності, підтвердження відповідності, метрологічного забезпечення діяльності, пов'язаної з вимірюванням фізичних величин, потребують вживання певних заходів з метою впорядкування системи технічного захисту інформації відповідно до вимог цих законів [9]. Усі ці чинники зумовлюють необхідність постійного розвитку всіх складових елементів системи технічного захисту інформації.

1. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, затверджений наказом ДСТСЗІ СБ України від 24.12.2001 р. №76 і зареєстрований у Міністерстві юстиції України 11.01.2002 р. за №27/6315 [Электронный ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/

show/z0027-02. **2.** Васильчак С. В. Порядок атестування системи технічного захисту інформації [Электронный ресурс] / С. В. Васильчак, С. В. Байдак // Науковий вісник НЛТУ України. – 2010. – № 14. – С. 333–337. – Режим доступу : http://firearticles.com/informaciyni-systemy/259-poryadok-atestuvannya-sistemi-tehnchnogo-zahistu-nformacyi.html. **3.** НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах [Электронный ресурс]. – Режим доступу : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=89740&cat_id= 89734. **4.** Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 № 567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175 [Электронный ресурс]. –Режим доступу : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=89740 &cat_id=89734. **5.** Положення про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 86, зареєстрований в Міністерстві юстиції України 04.06.2007 за № 577/13844 [Электронный ресурс]. – Режим доступу : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=89740&cat_id=89734. **6.** Фролов О. Система технічного захисту в Україні. Стан та перспективи розвитку / О. Фролов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2008. – Вип. L (16). – С. 12–14. **7.** Правила проведення робіт із сертифікації засобів захисту інформації. Спільний наказ Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 № 75/91, зареєстрований в Міністерстві юстиції України 14.05.2007 за № 98/13765 [Электронный ресурс]. – Режим доступу :http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_d=89740 &cat_id=89734. **8.** Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу [Электронный ресурс]. – Режим доступу : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=89740&cat_id=89734. **9.** Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ООО «ТИД ДС», 2004. – 992 с.