

ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

*Л.В. Борисова, к.ю.н., доцент, НУЦЗ України,
О.В. Закора, к.т.н., доцент, НУЦЗ України,
Є.Є. Селеєнко, НУЦЗ України,
А.Б. Феценко, к.т.н., доцент, НУЦЗ України*

Порядок організації діяльності підрозділів технічного захисту інформації в системі ДСНС України відповідно до наказу Міністерства України з надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 5 листоп. 2010 № 977 «Про організаційні засади діяльності підрозділів технічного захисту інформації у структурі МНС» визначає правові та організаційні засади діяльності підрозділів ДСНС, яким надано повноваження на проведення відповідних видів робіт з технічного захисту інформації в урядових органах державного управління, територіальних органах управління ДСНС, підприємствах, установах та організаціях, що належать до сфери управління ДСНС. Розв'язання завдань із захисту населення і територій від надзвичайних ситуацій неможливе без сучасної системи зв'язку, оповіщення та інформатизації ДСНС. Розпорядження Кабінету міністрів України «Про затвердження Комплексної програми розвитку системи зв'язку, оповіщення та інформатизації МНС на 2004-2010 роки» від 4 березня 2004 року № 109-р визначає основні завдання із захисту інформації:

- утворення підрозділів технічного захисту інформації (в тому числі в автоматизованих системах), регіональних лабораторій спеціальних досліджень, отримання у встановленому порядку ліцензій на виконання робіт у сфері криптографічного і технічного захисту інформації;
- забезпечення територіальних органів, підрозділів сил ДСНС спеціальною апаратурою, обладнанням і технічними засобами захисту;
- упровадження засобів захисту інформації з обмеженим доступом від просочення технічними каналами, програмних засобів антивірусного захисту в автоматизованих системах, програмно-апаратних засобів захисту від несанкціонованого доступу в автоматизованих системах, програмно-апаратних засобів криптографічного захисту в телекомунікаційних мережах;
- використання можливостей Національної системи конфіденційного зв'язку;
- проведення атестації комплексів технічного захисту інформації на об'єктах інформаційної діяльності;
- проектування комплексних систем захисту інформації в автоматизованих системах усіх рівнів;
- забезпечення захисту автоматизованих робочих місць, транспортних мереж передачі даних локальних обчислювальних мереж;
- упровадження програмно-апаратних засобів криптографічного захисту інформації в локальних обчислювальних мережах усіх рівнів;
- створення захищених систем електронного документообігу;
- проведення тестування комплексних систем захисту інформації з метою виявлення їх вразливості;

– проведення державної експертизи комплексних систем захисту інформації в автоматизованих системах.

Законом України від 23 лютого 2006 року № 3475-IV «Про державну службу спеціального зв'язку і захисту інформації України» у ст. 3 визначені основні задачі серед яких забезпечення у встановленому порядку урядовим зв'язком у мирний час, в умовах надзвичайного і воєнного положення, а також у випадках виникнення надзвичайних ситуацій. Згідно з наказом адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Положення про державний контроль за станом технічного захисту інформації» від 16 травня 2007 р. № 87, визначаються порядок організації та здійснення державного контролю за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога, щодо захисту якої встановлена законом.

Захист інформації від несанкціонованого доступу, а також криптографічний захист під час її передачі каналами системи зв'язку ДСНС здійснюється комплексно з урахуванням як новітніх технологій у телекомунікаційних системах, так і засобів (систем) несанкціонованого отримання інформації, її спотворення або знищення. Комплексні системи захисту інформації на об'єктах інформаційної діяльності від витоку технічними каналами створюються власними силами та із залученням організацій, що мають відповідні ліцензії (дозволи). Типове положення, про підрозділ, який виконує роботи з технічного захисту інформації в системі ДСНС визначає, що підрозділ технічного захисту інформації (підрозділ ТЗІ) є структурним підрозділом урядового органу державного управління, територіального органу управління ДСНС, а також підприємства, установи та організації, що належить до сфери управління ДСНС. Підрозділ ТЗІ – підрозділ Установи, призначений для виконання робіт з технічного захисту інформації в системі ДСНС відповідно до повноважень, наданих Міністерством згідно з Дозволом на проведення робіт з технічного захисту інформації для власних потреб.

Види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ:

1. Розроблення, впровадження, випробування, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля.
2. Розроблення, впровадження, випробування, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали.
3. Розроблення, впровадження, випробування, супроводження комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу.
4. Виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності.

ЛІТЕРАТУРА

1. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99 (1229/99).
2. Типовий порядок створення комплексних систем захисту інформації в автоматизованих системах класу 1 у структурі МНС України, погоджений з Держспецзв'язку 22.05.2007 і затверджений наказом МНС від 08.08.2007 № 539дск.