особового складу ЗС України та поступове їх поєднання в єдину автоматизовану систему підготовки (АСП) ЗС України. АСП ЗС України є складовою частиною єдиної автоматизованої системи управління ЗС України і призначається для динамічного централізованого управління підготовкою ЗС України та дистанційного виконання заходів військового навчання. АСП ЗС України має забезпечити: автоматизоване перспективне планування підготовки; автоматизоване короткострокове планування підготовки з урахуванням рівня підготовки; застосування систем дистанційного навчання, створення єдиної методичної та інформаційної бази системи підготовки. Попередні розрахунки показують, що при впровадженні АСП ЗС України автоматизоване рішення оптимізаційних задач розподілу ресурсів та планування заходів дозволить: збільшити кількість ресурсно забезпечених заходів підготовки при фіксованій кількості ресурсів в середньому на 15 %; зекономити близько 27 % ресурсів, що необхідні для проведення фіксованого числа заходів підготовки; зменшити тривалість циклу планування підготовки військ (сил) ЗС України приблизно в 10 разів. На першому етапі розробки та впровадження АСП ЗС України потребують вирішення близько 3200 функціональних задач.

ПЕРСПЕКТИВНА СИСТЕМА ВИЯВЛЕНННЯ ВТОРГНЕНЬ У ІНФОРМАЦІЙНІ МЕРЕЖІ

І.В. Рубан, д.т.н., проф.; Д.В. Прибильнов
Харківський університет Повітряних Сил імені Івана Кожедуба

На сучасному етапі розвитку інформаційно-обчислювальних мереж як ніколи актуальним постає питання захисту та виявлення несанкціонованого вторгнення або використання інформаційної мережі. Спираючись на існуючі публікації [1], можна стверджувати, що системи виявлення вторгнень є широковживаними при регулюванні аспектів захисту інформації. Сучасний рівень їх розвитку дозволяє з гарантованою імовірністю виявляти відомі класи атак[2]. Але дані системи не здатні гарантовано забезпечити виявлення не класифікованих інформаційних загроз. Залишається висока імовірність хибного виявлення або пропуску атак, що не були розглянуті експертами, тобто на які не було складено сигнатур. Дані факти вимагають створення систем виявлення вторгнень, що ґрунтуються на несигнатурних принципах виявлення. Одним із таких принципів є моніторинг мережевої активності користувачів. Пропонується вести безперервний моніторинг шляхом аналізу інформації, що надходить від агентів мережі. Під агентами розуміється спеціальне програмне забезпечення, що встановлено на кожному робочому місці користувача і веде безперервне спостереження за входженням у мережу та використанням її ресурсів. Аналіз відбувається на робочому місці адміністратора із використанням навченої нейронної мережі. У якості додаткового інструментарію пропонується використати вейвлет-аналіз. Запропонована методика дозволить виявляти несигнатурні атаки.

МАТЕМАТИЧНА МОДЕЛЬ ДІЙ ПОВІТРЯНОГО ПРОТИВНИКА

М.М. Ігнатьєв
Центральний науково-дослідний інститут Збройних Сил України

У сучасних умовах математичне моделювання є одним з основних інструментальних засобів досліджень за проблематикою будівництва, застосування, всебічного забезпечення та управління ЗС України. У провідних країнах світу