УДК 623. 765:681.513.6 **doi: 10.26906/SUNZ.2019.3.110**

В. В. Кальченко

Національний аерокосмічний університет імені М.Є. Жуковського "ХАІ", Харків, Україна

АНАЛІЗ ІСНУЮЧОЇ МЕТОДИКИ ПРОВЕДЕННЯ АУДИТУ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ В ДЕРЖАВНИХ ОРГАНАХ

Предметом статті є аналіз існуючих методик проведення аудиту безпеки, які нормативно закріплені в Україні та використовуються посадовими особами Державної служби спеціального зв'язку та захисту інформації України. **Результати**. Проаналізовано існуючу методику проведення перевірок захищеності інформації в інформаційно-телекомунікаційних системах державних органів, органів місцевого самоврядування, підприємств установ та організацій. Враховуючи недоліки існуючої системи проведення перевірок з захисту інформації та введенням в дію Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року № 2163-VIII запропоновано підходи до проведення перевірок кіберзахисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлено законодавством. **Висновок.** Обгрунтована необхідність розробки методології визначення реального стану захищеності інформаційних систем, в яких циркулює інформація, що потребує захисту згідно вимог законодавства України.

Ключові слова: тестування на проникнення, пентестінг, кібербезпека, кіберзахист.

Вступ

Конституція України проголошує, що «забезпечення … інформаційної безпеки є найважливішими функціями держави» [1]. Це досягається за рахунок властивості системи в перебігу заданого часу протистояти несанкціонованому зняттю і модифікації інформації [2]. При цьому забезпечується конфіденційність, цілісність і доступність інформації. Якщо питань забезпечення конфіденційності фахівцями в області інформаційної безпеки приділяється досить багато уваги, то питання забезпечення цілісності та доступності вимагають серйозного опрацювання. Методи забезпечення цілісності та доступності багато в чому перетинаються. Це резервування інформації, надійність технічної складової, наявність надійних і дубльованих каналів передачі інформації [3, 4]. Разом з тим збігаються і загрози цим властивостям. Це в першу чергу деструктивні дії, результатом яких є неможливість отримати неспотворену інформацію або взагалі її незнаходження. Це протиборство двох начал особливо яскраво проявляється в кіберпросторі, в якому воно виходить на новий рівень протистояння. На даний час в Україні гостро постало питання створення системи кібербезпеки, яка повинна забезпечити виявлення нових і невідомих кіберзагроз та кібератак в ході моніторингу кіберпростору, аналізу виявлених кіберзагроз (кібератак), автоматичний вибір параметрів функціонування інформаційних систем і мереж зв'язку в умовах деструктивних впливів.

Протиборство країн вимагає проведення розвідки в кіберпросторі з подальшим цифровим проникненням в мережі і системи управління потенційного противника і передбачає використання абсолютно нових джерел, форм і способів збору даних та інформації, розробки нових розвідувальних засобів і технологій, тактичних і технічних прийомів. Для попередження і мінімізації деструктивного впливу кіберзагроз створюються відповідні системи захисту. Проте виникає проблема оцінки того, наскільки якісно система захисту може протидіяти загрозам. На момент написання статті в Україні наявний лише один нормативний документ який в якому прямо йде мова про кібербезпеку та протидію кіберзагрозам, а саме [5]. Цей нормативний документ визначає правові та організаційні основи забезпечення безпеки в кіберпросторі, та визначає поняття критичної інфраструктури. Варто зазначити, що даний документ є першим національним нормативним документом з цієї тематики, має декларативний характер та не містить чітких вимог до інформаційних систем.

Метою даної статті є аналіз існуючої системи аудити безпеки інформаційних систем та вироблення нових підходів до проведення оцінювання захищеності комп'ютерних систем через застосування тестування на проникнення.

Результати досліджень

1. Огляд законодавства в сфері проведення перевірок захищеності інформації в комп'ютерних системах. Під аудитом інформаційної безпеки інформаційних систем розуміють процес одержання об'єктивної, якісної та кількісної оцінок поточного стану безпеки комп'ютерної системи, отримання комплексної оцінки рівня інформаційної безпеки. Необхідність проведення регулярного аудиту інформаційної безпеки полягає в здійсненні оцінки реального стану захищеності інформаційних ресурсів в комп'ютерній системі та перевірки спроможності системи безпеки протидіяти сучасним загрозам, які постійно змінюються та вдосконалюються. В нашій країні аудит інформаційної безпеки державних органів реалізується шляхом проведення перевірок стану технічного захисту інформації (ТЗІ).

На даний час основними документами, які регулюють питання пов'язані з захистом інформації в інформаційно-телекомунікаційних системах є [6, 7]. Згідно даних нормативних документів, основною вимогою до інформаційних систем з точки зору безпеки – є наявність в них побудованої комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. При цьому необхідність побудови КСЗІ визначається типом інформації, що циркулює в даній системі. Такими видами є секретна інформація,

службова інформація, конфіденційна інформація (наприклад персональні дані) та державні інформаційні ресурси. Порядок побудови та вимоги до цих систем визначаються нормативними документами системи технічного захисту інформації (НД ТЗІ). Згідно [8] головним регулятором в області інформаційної безпеки є Державна служба спеціального зв'язку та захисту інформації України. Згідно даного нормативного акту служба не тільки встановлює вимоги з захисту інформації, але і проводить перевірки стану захищеності систем. Свою діяльність з перевірок захисту інформації в комп'ютерних системах, державний регулятор здійснює на підставі [9, 10].

2. Аналіз існуючої моделі проведення перевірок стану ТЗІ в комп'ютерних системах державних органів. Перевірки стану ТЗІ здійснюється посадовими особами регіональних управлінь Держспецзв'язку. Основним документом, який регламентує проведення даних заходів є [9]. Згідно даного документу національна процедуру проведення аудиту інформаційної безпеки складається з 6 етапів:

1. Вивчення загальних питань. На даному етапі з'ясовується юридична назва установи, її адреса, структура, основні завдання діяльності, умови розташування, пропускний режим, наявність систем захисту, тощо.

2. Аналіз заходів з захисту інформації з обмеженим доступом (ІзОД), розголошення якої може призвести до негативних наслідків як для установи в цілому, так і для окремих її робітників.

3. Аналіз заходів з ТЗІ, що циркулює в комп'ютерних системах, засобах розмноження документів, та інших пристроях.

4. Аналіз заходів з ТЗІ при створенні різноманітної продукції або технологій для державних потреб, при виконанні науково-дослідних, дослідно-конструкторських робіт в державних інтересах.

5. Аналіз заходів з ТЗІ під час проведення проектування, будівництва, реконструкції або капітального ремонту ОІД.

6. Аналіз заходів з технічного захисту ІзОД під час прийому іноземних делегацій.

Враховуючи мету статті, розглянемо більш детально третій етап, а саме аналіз заходів з ТЗІ в інформаційних, інформаційно-телекомунікаційних системах (ІТС). На даному етапі:

– визначаються комп'ютерні системи в яких циркулює інформація, що потребує захисту згідно законодавства України;

– з'ясовується питання щодо наявності створених КСЗІ в даних системах;

– визначаються посадові особи відповідальні за захист інформації в установі в цілому, та в окремих комп'ютерних системах;

– перевіряються дані зазначені в технічний та експлуатаційній документації на КСЗІ реальним умовам розташування та функціонування кожної комп'ютерної системи та системи безпеки;

– визначаються типи інформації яка циркулює в комп'ютерної системи, що оцінюється, та проходить визначення програмних засобів що використовуються для її обробки;

– перевіряється комплектність технічної та експлуатаційної документації на КСЗІ, та її відповідність вимогам НД ТЗІ;

– перевіряється працездатність засобів захисту всіх складових комп'ютерної системи;

– перевіряється наявність антивірусу та періодичність його оновлення;

– перевіряється коректність налаштування засобів захисту в комп'ютерних системах. Як правило, для комп'ютерної системи з кількістю робочих станцій більше 10 штук, в якості засобів захисту виступають сервіси безпеки операційної системи Windows. Враховуючи даний факт, здійснюється порівняння налаштувань серверів та робочих станцій з вимогами, які висуваються в відповідних інструкціях, що входять до складу документації на КСЗІ; перевіряється виконання умов експлуатації комп'ютерної системи, які зазначені в експертному висновку на КСЗІ; складається звіт де визначається повнота та достатність заходів з ТЗІ і визначається відповідність КСЗІ вимогам нормативно-правових актів. При цьому варто зазначити, що перевірка налаштувань параметрів безпеки здійснюється відповідно до інструкцій (настанов), які були розроблені організацією, що створювала КСЗІ. В разі відсутності системи захисту, перевірка налаштувань параметрів безпеки не здійснюється через фізичну відсутність еталонного документу з яким необхідно порівнювати поточні налаштування системи. За результатами перевірки складається акт, в якому надаються рекомендації (вимоги) щодо приведення стану ТЗІ у відповідність до вимог законодавства України, а саме створення КСЗІ. Крім того надаються рекомендації щодо розробки певних документів, необхідних для створення та впровадження КСЗІ. Прикладами таких заходів є: створення комісії та проведення категорію вання комп'ютерів на яких здійснюється обробка ІзОД; створення комісії та проведення обстеження функціонування комп'ютерної системи; аналіз інформаційної діяльності установи та складання моделі загроз, моделі порушника для інформації; розробку політики безпеки; складання плану захисту інформації; розробки технічного завдання на створення КСЗІ та погодження його з Адміністрацією Держспецзв'язку.

Проте конкретних рекомендацій стосовно конфігурування параметрів безпеки операційних систем, конфігурування мережевого обладнання, тощо, акти перевірок не містять. Це пов'язано з тим, що НД ТЗІ не містять ніяких рекомендацій з цих питань. Як наслідок у посадових осіб Держспецзв'язку немає правових підстав для надання рекомендацій, які безпосередньо впливають на фактичну захищеність комп'ютерної системи.

Варто зазначити, що керівництвом Держспецзв'язку були зроблені кроки в напрямку організації проведення перевірок фактичної захищеності комп'ютерних систем. Результатом таких кроків стало розроблення та ухвалення нормативного документу [10]. Фактично даний вид оцінки є тестом на проникнення (penetration test, pentest). Тест на проникнення це симуляція атаки на систему, мережу, частину обладнання чи інші засоби обслуговування, з ме-

тою доказу того, наскільки ця система вразлива для реального нападу. Процес тестування максимально схожий на процес злому, який проводить зловмисник. В ході тесту відповідний фахівець (група фахівців) намагається отримати доступ до інформації, яка обробляється в комп'ютерній системі, отримати контроль над роботою системи, або вивести її з ладу. Такий фахівець (пентестер) виступає в ролі злодія, і намагається з'ясувати найбільш вразливі місця в системі, зафіксувати їх в звіті і передати відповідним працівникам організації-замовника для усунення. Під час проведення тесту йде визначення того, як система реагує на атаку (в незалежності від того можливо чи ні порушити захист системи) і яку інформацію можна отримати в системі. За результатами проведених робіт власник системи отримує звіт в якому вказуються недоліки в системі інформаційної безпеки підприємства та надаються практичні рекомендації щодо усунення виявлених вразливостей. Такий тип перевірок проводиться лише одним підрозділом Держспецзв'язку, а саме CERT-UA (Computer Emergency Response Team of Ukraine - Команда реагування на комп'ютерні надзвичайні події України), який фізично дислокується в м. Києві (https://cert.gov.ua/). Враховуючи кількість державних органів, підприємств та організацій, а також об'єктів критичної інфраструктури даний факт не дозволяє в повному обсязі здійснювати перевірки на всіх зацікавлених державних установ. Враховуючи досвід автора з проведення перевірок стану ТЗІ та аналізу нормативних документів в цій сфері, можна виділити дві основні проблеми існуючої методики проведення аудиту безпеки інформаційних систем в нашій країні [11]:

- відсутні методології проведення пентестінгу та документів, які б давали рекомендації щодо підвищення рівня захищеності інформації. Враховуючи зміст та вимоги «Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах», затвердженого Адміністрацією Держспецзв'язку від 02.12.2014 №660, дана оцінка проводиться посадовими особами Держспецзв'язку виходячи з їх знань, умінь та суб'єктивних суджень;

- побудовою систем захисту інформації в більшості своїй займаються невеликі за чисельністю приватні суб'єкти господарювання, що мають ліцензію, видану Адміністрацією Держспецзв'язку. Враховуючи цей фактор, а також недосконаліть НД ТЗІ на практиці виникає ситуація, коли один або декілька співробітників фірм-ліцензіатів приймають одноосібне рішення щодо конфігурування параметрів безпеки комп'ютерних систем. Таким чином, рішення приймається не на основі вимог нормативних документів, висновків наукових досліджень або експериментів, а лише на основі суб'єктивної думки зазначених осіб. При цьому з правової точки зору, посадовим особам Держспецзв'язку досить складно поставити під сумнів (опротестувати) конфігурацію системи захисту інформації.

Одним з варіантів вирішення даної проблеми було проведення тестування на проникнення відповідно до затвердженої методології, що б дало змогу провести оцінку отриманих результатів. Проте варто констатувати, що необхідність обов'язкового проведення тестів на проникнення після побудови КСЗІ, на даний час нормативно не закріплена. Таким чином, в нашій країні побудова КСЗІ зводиться до правильного написання технічної та експлуатаційної документації, а державна експертиза - до перевірки правильності написання вищезазначених документів. Для об'єктивності варто зазначити, що процес погодження ТЗ передбачає аналіз заходів з захисту інформації. Проте опис системи може бути зроблений неправильно, що в свою чергу може призвести до неправильної оцінки фахівцями Держспецзв'язку вибраного профілю захищеності і вимог, які висуваються до системи.

Таким чином замовник отримує умовно захищену систему, яка не може протидіяти сучасним загрозам, але має необхідний перелік дозвільних документів (Атестат відповідності та експертний висновок про відповідність КСЗІ вимогам НД ТЗІ),

Також проблемним питанням є той факт, що при наявності в установі it-відділу або відділу інформаційної безпеки, вони не можуть підтвердити достатність вжитих заходів з безпеки шляхом проведення відповідної державної експертизи. При цьому сама процедура проведення такої експертизи потребує виділення значних грошових коштів. Враховуючи хронічне недофінансування робіт з захисту інформації, виникають парадоксальні ситуації: з одного боку існують комп'ютерної системи, параметри безпеки яких налагоджені відповідно до рекомендацій провідних компаній з інформаційної безпеки, з іншої сторони для того щоб це підтвердити – необхідно сплатити грошові кошти комерційній структурі з відповідною ліцензією, фахівці якої можуть мати меншу кваліфікацію, проте зроблять необхідний висновок. Таким чином Атестат відповідності на автоматизовану систему класу «3» отримати неможливо.

3. Шляхи вирішення проблеми захисту інформації в національних комп'ютерних системах. Можливим варіантом вирішення даної проблеми може бути розробка національної методології проведення тестування на проникнення та впровадження (на законодавчому рівні) механізму підтвердження захищеності інформації за результатами проведення відповідного тестування фахівцями Держспецзв'язку.

Як зазначалось вище, процес тестування максимально схожий на процес злому, який проводить зловмисник. В ході тесту, група фахівців (так званих етичних хакерів) намагається порушити одне або декількох з трьох основних властивостей інформації, що обробляється в системі: конфіденційності, цілісності, доступності. Фактично, в ході тесту з'ясовуються, яким чином можна скомпрометувати цільову систему. При належному проведенні тестування, власник комп'ютерної системи отримує незалежну оцінку захищеності інформації в даній системі. В залежності від результатів можна проводити заходи з модернізації системи безпеки в цілому або вжиття більш доцільних заходів з безпеки, враховуючи розвиток засобів проникнення інформаційних систем.

Розглядаючи питання розробки національної методології тестування на проникнення, можна спи-

ратись на досвід провідних компаній світу та загально прийнятих методологій з цього питання. Можна виділити декілька найбільш розповсюджених методологій проведення тестування на проникнення, а саме: The Open Source Security Testing Methodology Manual (OSSTMM) [12]; The National Institute of Standards and Technology (NIST) Special Publication 800-115[13]; OWASP Testing Guide [14]; Penetration Testing Execution Standard (PTES) [15]; Information Systems Security Assessment Framework (ISSAF) [16].

Короткий опис даних методологій наведено в [11]. Кожна з даних методологій має свої недоліки та переваги. Проте використовуючи їх, можна розробити національну методологію, яка буде поєднувати всі переваги і враховувати особливості українського законодавства, розвиток національних комп'ютерних систем, їх особливостей, тощо [17, 18].

Розглядаючи необхідність розробки методології тестування на проникнення, варто зазначити, що кожна комп'ютерна система – є унікальною. Наприклад: одна система може будуватись на основі операційних систем Windows від корпорації Microsoft, інші – на основі багаточисельних версій Linux. Для обробки «чуттєвої» інформації можуть використовуватись не тільки стандартні програмні засоби Microsoft Office, OpenOffice, LibreOffice, але й спеціалізовані системи документообігу (наприклад FossDoc, АСКОД, Optima-WorkFlow-Стандарт, тощо). Також варто зазначити, що інформація може циркулювати в спеціалізованих, розподілених інформаційних системах. Прикладами таких систем можуть бути: інтегрована міжвідомча автоматизована система обміну інформацією щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон України (Гарт-1), що використовується Державною прикордонною службою України [19]; автоматизована інформаційна система «Податковий блок» Державної фіскальної служби України [20]; єдина інформаційна система Міністерства внутрішніх справ України [21]. В свою чергу це потребує розробки вузькоспеціалізованих методів тестування. Враховуючи вищезазначене, методологія тестування на проникнення повинна будуватись за модульним принципом. Кожен модуль – це деякий алгоритм тестування конкретної операційної системи, програмного продукту, підсистеми в цілому. Наприклад: алгоритм тестування контролеру домену, системи керування базами даних, поштового серверу, серверу терміналів, Web, DNS, DHCP серверів, робочих станцій, тощо.

В загальному випадку процедуру проведення тестування пропонується поділити на 5 основних модулів: визначення об'єктів захисту, збір початкової інформації про цільову систему; визначення області дослідження, складання моделі загроз; пошук та визначення вразливостей; експлуатація вразливостей, проникнення в систему та пошук можливостей порушення одного або декількох властивостей «чутливої» інформації; складання звітних матеріалів.

Використання модульного принципу дозволить періодично оновлювати кожен модуль без затвердження, погодження всієї методології в цілому, що важливо з точки зору економії часу коли річ йде про національні нормативні акти.

Висновок

Сучасні темпи розвитку комп'ютерної техніки, проведення спецслужбами, організованими кримінальними угрупованнями операцій у кіберпросторі потребують оперативного реагування на інциденти інформаційної безпеки зі сторони відповідних фахівців державних органів та впровадження сучасних засобів захисту інформації. Існуюча система побудови систем захисту комп'ютерних мереж морально застаріла і не відповідає викликам сучасності. В свою чергу методика проведення аудиту (перевірок) безпеки комп'ютерних систем в Україні також не відповідає міжнародним, загальноприйнятим стандартам. Сам принцип побудови та експлуатації КСЗІ не дає змоги оперативне реагувати та усувати програмні та апаратні вразливості, які стали загальновідомими. Це пов'язано з тим, що як будь-які зміни в налаштуваннях комплексу засобів захисту комп'ютерної системи потребують проведення додаткової державної експертизи. Внаслідок цього звичайні вразливості для комп'ютерних систем державних органів перетворюються на вразливості нульового дня. Звичайно для вирішення даної проблематики необхідно залучати міжнародні інституції, досвідчених фахівців та насамперед вносити зміни в законодавство в сфері захисту інформації. Проте з технічної точки зору, можливим методом підвищення реальної захищеності комп'ютерних систем – є періодичне проведення тестування на проникнення. Перевагою такого методу є визначення реальної захищеності, невисока вартість його проведення, та надання відповідним фахівцям (системним адміністраторам) практичних рекомендацій з налаштування параметрів безпеки комп'ютерних систем.

СПИСОК ЛІТЕРАТУРИ

1. Конституція України: офіц. .текст. Київ: КМ, 2013.93 с.
2. Певнев В.Я., Цуранов М.В. Математическая модель информационной безопасности. *Системи обробки інформації.* 2010. №3. С. 62-64
3. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. *Економіка і організація управління* 2014. № 1-2. С. 54-60
4. Певнев В.Я. Методы обеспечения целостности информации в инфокоммуникационных системах. *Вісник Національного технічного університету ХПІ. Серія: Техніка та електрофізика високих напруг.* Харків, 2015. № 51. С. 74-77
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2469-VIII від 21.06.2018, *ВВР*, 2018, № 31, ст.241
6. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України» від 05.07.1994. № 1170-VII (1170-18) від 27.03.2014, *ВВР*, 2014, N 22, ст.816

7. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Постанова Кабінету Міністрів України від 29.03.2006 р. №373 Офіційний вісник України 2006 р., № 13, стор. 164
8. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України» №3475-IV від 23.02.2006 № 2163-VIII від 05.10.2017, *ВВР*, 2017, № 45, ст.403
9. Про затвердження Положення про державний контроль за станом ТЗІ. Наказ Адміністрації Держспецзв'язку від 16.05.2007 №87
10. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Наказ Адміністрації Держспецзв'язку від 02.12.2014 №660
11. Кальченко В.В. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем. *Системи управління, навігації та зв'язку*. 2018. №4 . С. 109-114
12. The Open Source Security Testing Methodology Manual (OSSTMM). [Електронний ресурс]. – Режим доступу: http://www.isecom.org/mirror/OSSTMM.3.pdf (дата звернення: 27.03.2019)
13. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Special Publication 800-115. [Електронний ресурс]. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата звернення: 27.03.2019)
14. OWASP Testing Guide v4. [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/OWASP_Testing_Project (дата звернення: 27.03.2019)
15. The Penetration Testing Execution Standard (PTES). [Електронний ресурс]. – Режим доступу: http://www.pentest-standard.org/index.php/Main_Page (дата звернення: 27.03.2019)
16. Information Systems Security Assessment Framework (ISSAF). [Електронний ресурс]. – Режим доступу: http://www.oissg.org/files/issaf0.2.1.pdf (дата звернення: 27.03.2019)
17. Kuchuk G., Nechausov S., Kharchenko, V. Two-stage optimization of resource allocation for hybrid cloud data store. *International Conference on Information and Digital Technologies. Zilina*, 2015. P. 266-271. DOI: http://dx.doi.org/10.1109/DT.2015.7222982
18. Kuchuk G.A. An Approach To Development Of Complex Metric For Multiservice Network Security Assessment / G.A. Kuchuk, A.A. Kovalenko, A.A. Mozhaev // Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010.– Kiev: NAU, RED, IEEE Ukraine section joint SP, 2010. – P. 158 – 160.
19. «Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України. Наказ Адміністрації Державної прикордонної служби України від 20.09.2008 №810
20. Про введення в експлуатацію інформаційної системи «Податковий блок». Наказ ДПС України № 1197 від 24.12.2012
21. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів. Постанова Кабінету Міністрів України від 14.11.2018 р. №1024 Урядовий кур'єр офіц.. видання. 2018. 12 (№ 235)

Рецензент: д-р техн. наук, проф. І. В. Шостак,
Національний аерокосмічний університет "ХАІ", Харків
Received (Надійшла) 20.03.2019
Accepted for publication (Прийнята до друку) 25.04.2019

Анализ существующей методики проведения аудита безопасности компьютерных систем в государственных органах

В. В. Кальченко

Предметом статьи является анализ существующих методик проведения аудита безопасности, нормативно закреплены в Украине и используются должностными лицами Государственной службы специальной связи и защиты информации Украины. **Результаты**. Проанализирована существующая методика проведения проверок защищенности информации в информационно-телекоммуникационных системах государственных органов, органов местного самоуправления, предприятий, учреждений и организаций. Учитывая недостатки существующей системы проведения проверок по защите информации и введением в действие Закона Украины «Об основных принципах обеспечения кибербезопасности Украины» от 05.10.2017 года № 2163-VIII предложены подходы к проведению проверок киберзащиты государственных информационных ресурсов и информации, требование относительно защиты которой установлено законодательством. **Вывод.** Обоснована необходимость разработки методологии определения реального состояния защищенности информационных систем, в которых циркулирует информация, что нуждается в защите в соответствии с требованиями законодательства Украины.

Ключевые слова: тестирование на проникновение, пентестинг, кибербезопасность, киберзащита.

Analysis of existing methods of audit of safety of computer systems in public authorities

V. Kalchenko

The subject of the article is an analysis of existing methods of conducting an audit of safety, which are regulated in Ukraine and used by officials of the State Service for Special Communications and Information Protection of Ukraine. **Results** An existing method of conducting inspections of information security in information and telecommunication systems of state bodies, local self-government bodies, enterprises of institutions and organizations has been analyzed. Taking into account the shortcomings of the existing system of information security inspections and the enactment of the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" dated 10/5/2017, No. 2163-VIII, the approaches to conducting cyber defense checks of state information resources and information, the requirement for protection of which is established by law, is proposed. **Conclusion**. The necessity of developing a methodology for determining the real state of the security of information systems in which circulating information that needs protection in accordance with the requirements of Ukrainian legislation is substantiated.

Keywords: penetration testing, pentesting, cyber security, cyber defense.