УДК 004.056

В.Л. Бурячок[1]

[1]Начальник науково-дослідного управління військової частини А1906, д.т.н., старший науковий співробітник

СУЧАСНІ СИСТЕМИ ВИЯВЛЕННЯ АТАК В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ. МОДЕЛЬ ВИБОРУ РАЦІОНАЛЬНОГО ВАРІАНТА РЕАГУВАННЯ НА ПРОЯВИ СТОРОННЬОГО КІБЕРНЕТИЧНОГО ВПЛИВУ

У статті зважаючи на масштаби застосування сучасних інформаційно-комунікаційних технологій та проблеми, пов'язані із забезпеченням продуктивності, надійності та стійкості функціонування інформаційно-телекомунікаційних систем, а також захисту від несанкціонованого доступу циркулюючих у таких системах інформаційних ресурсів розглянуто підхід до формування моделі вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу.

Ключові слова: ІТ системи, СІТС, мережа, хост.

Постановка завдання у загальному вигляді. Сучасний етап у розвитку теорії і практики обміну інформацією характеризується головним чином інтенсивним впровадженням нових інформаційно-комунікаційних технологій (ІКТ) та інформаційно-телекомунікаційних (ІТ) систем, зростанням кількості та високою технологічністю нових засобів і методів деструктивного впливу на об'єкти інформаційної діяльності (ОІД), а також підвищенням професіоналізму потенціальних порушників – неавторизованих користувачів, інсайдерів, хакерів, крекерів тощо. Нині такий стан справ простежується практично на усіх рівнях ієрархії, починаючи з архітектурного рівня Internet та Intranet у цілому, включаючи мережеві технології (мережеве програмне забезпечення тощо) й закінчуючи рівнем загальносистемних засобів і додатків (ОС, СУБД тощо).

Зважаючи на те, що масштаби застосування сучасних ІКТ останнім часом розширились до практично неосяжних меж поряд із проблемами забезпечення продуктивності, надійності та стійкості функціонування ІТС це визначило також й проблему захисту від несанкціонованого доступу (НСД) циркулюючих у таких системах інформаційних ресурсів (ІР). З одного боку ця проблема обумовлюється, як відомо, посиленою увагою до безпеки ІТС, а з іншого – неухильно зростаючими збитками, які порушники завдають власникам ІР. Вирішити її, як показує статистика, можна нині використовуючи засоби захисту убудовані в операційні системи (ОС) і додатки або застосовуючи поряд з убудованими додаткові захисні програмно-апаратні механізми.

Аналіз останніх досліджень і публікацій. Означену проблему висвітлено в багатьох публікаціях зарубіжних і вітчизняних авторів. Найвідомішими серед них є роботи К. Касперски, М. Левіна, С. Мак-Клара, Дж. Скембрея, Д. Фері, Б.Ю. Аніна, С.В. Ленкова, Д.В. Склярова, В.О. Хорошка та інших фахівців. Тим не менш аналіз публікацій у предметній області, що розглядається, свідчить про те, що комплексне дослідження проблеми, перш за все інформаційної та кібербезпеки ІР, методів, які при цьому

застосовуються, а також їх особливостей на цей час практично відсутнє. Тому, враховуючи реалії сьогодення, вона потребує додаткового і більш глибокого вивчення.

Актуальність та мета статті. Отже, актуальність статті зумовлено передусім обсягом інформації, що останнім часом надходить до користувачів із зовнішнього середовища та безперервно зростає, а також потребою підвищення результативності захисту інфосфери України від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз. Метою статті є формування зрозумілого, науково-обґрунтованого понятійного апарату в цій предметній області, а також моделі вибору раціонального варіанта реагування на події порушення безпеки в ІТ системах і мережах.

Виклад основного матеріалу. Наприкінці XX – початку XXI сторіччя завдяки глибоким системним перетворенням, викликаним синтезом перспективних ІКТ та бурхливим розвитком ІТ систем і мереж у світі та Україні зокрема суттєво активізувалась робота за напрямами:

виявлення інформаційних потреб та добору джерел інформації;

пошуку та збору інформації у відкритих і відносно-відкритих, а також її добування із закритих електронних джерел;

опрацювання інформації, оцінювання її повноти і значущості;

подання інформації у зручному для користувачів вигляді та організації зворотного зв'язку з нею;

використання інформації для оцінювання тенденцій, розробки прогнозів, оцінювання альтернатив рішень і дій, вироблення стратегій тощо.

Цьому сприяло створення спеціальних ІТ систем (СІТС), що мали високі споживчі якості та були здатні реалізовувати певні обчислювальні, відслідковувальні, запам'ятовувальні, комунікаційні, інформаційні, регулювальні, оптимізаційні, прогнозні, аналітичні та документувальні функції. З урахуванням положень [1, 2] під СІТС будемо розуміти сукупність інформаційних та телекомунікаційних систем, що складаються з ряду взаємозалежних функціональних елементів – підсистем та їх окремих компонент, орієнтованих на виконання визначених функцій і завдань та які у процесі обробки інформації діють як єдине ціле. Мета їх створення полягає в тому, щоб у гранично короткі терміни створити систему обробки даних, яка має забезпечити їх інформаційну і кібернетичну безпеку. При цьому кібернетична безпека СІТС [3] має бути спрямована на забезпечення своєчасного виявлення реальних і потенційних, фактично неприхованих викликів, кібернетичних втручань і загроз випадкового або навмисного, природного або штучного характеру, а також запобігання спробам впливу на нормальний процес функціонування таких систем на різних етапах їх життєвого циклу, а інформаційна [3] – на протидію спробам одержання, всупереч установленим правилам, доступу до інформації, що циркулює в СІТС, її несанкціонованого поширення, модифікації або руйнування, порушення процедур ідентифікації та аутентифікації користувачів і процесів тощо.

Через високу складність і дорожнечу розробки захищених СІТС з часом з'явився й почав активно розвиватися напрямок інформаційної безпеки, пов'язаний з виявленням стороннього кібернетичного впливу проти таких систем. Поступово він одержав єдину узагальнену назву – "система виявлення атак" (СВА) й був орієнтований на реалізацію таких основних функцій [4, 5]:

збір даних про значення контрольованих ознак;

виявлення та ідентифікація несанкціонованих дій;

реагування на вторгнення з метою блокування його розвитку.

Сучасні СВА передбачають виявлення і фіксацію усіх зловживань та аномалій, починаючи зі входу до СІТС, включення комплексу засобів забезпечення безпеки з метою перевірки конфіденційності, цілісності та доступності інформації, повноважень користувачів та аналізу збоїв, а також реагування на події порушення безпеки СІТС з метою блокування їх розвитку. При цьому головне завдання засобів, що реалізують техно-

логії виявлення атак полягають в тому, щоб автоматизувати усі функції управління захистом СІТС та зробити їх зрозумілими для користувачів. Враховуючи таке типова архітектура моделі виявлення атак може бути представлена схемою, наданою на рис. 1. Схема поєднує у собі мережеві і хостові засоби збору інформації (сенсори), а також засоби реагування та засоби управління [6]. При цьому мережеві сенсори (Network IDS, NIDS) згідно наведеної схеми здійснюють перехоплення мережевого трафіку та розпізнавання атак. Для цього використовуються, як правило, методи:

виявлення відповідності трафіка певному шаблону (сигнатурі), виразу або байткоду, що характеризують атаку;

проведення контролю частоти подій або певної порогової величини;

проведення кореляції декількох подій з низьким пріоритетом;

виявлення статистичних аномалій тощо.

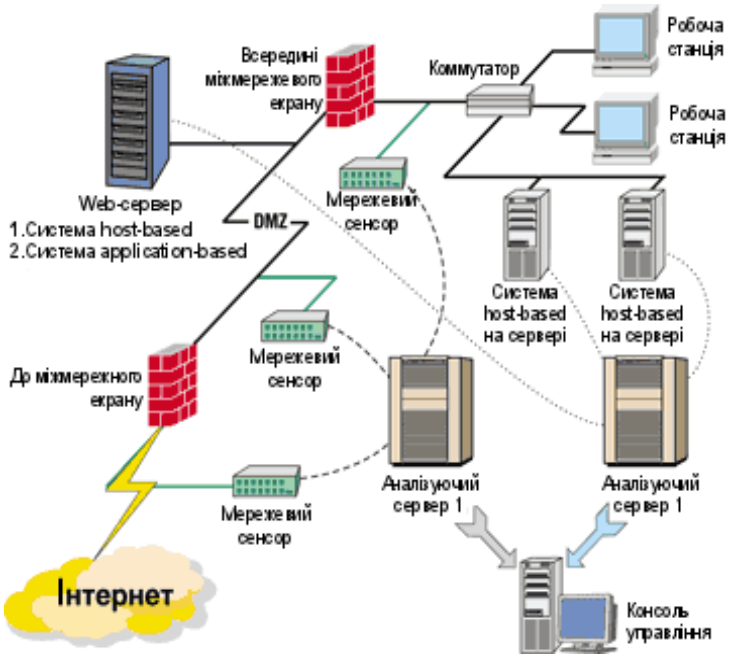

Рис. 1. Типова схема системи виявлення атк

Типовим прикладом мережевого сенсору може бути система, що контролює кількість TCP-запитів на з'єднання (SYN) з багатьма портами на обраному комп'ютері, виявляючи при цьому сканування TCP-портів. Звичайні користувачі використовують для цього RealSecure Network Sensor компанії Internet Security System (ISS), NetProwler компанії AXENT або Snort – вільно розповсюджувану систему виявлення атак з відкритим вихідним кодом. Більш спеціалізованими є продукти компаній Cisco та Internet Security System. Серед головних переваг мережевих сенсорів слід відзначити їх можливість щодо: ідентифікації атак перш, ніж вони досягнуть своєї мети; контролю великої кількості вузлів без зниження продуктивності всієї мережі; виявлення окремих видів атак, які "пропускають" хостові сенсори, невдалих атак або підозрілих намірів; виявлення й реагування на виявлені атаки у реальному масштабі часу; незалежності від типу ОС, а також низьку вартість експлуатації. До їх недоліків слід віднести наявність обмежень з виявлення атак, розподілених за часом та атак у сильно завантажених сегментах мережі.

Хостові сенсори (host-based intrusuon detection system) встановлюються на окремому вузлі (сервері) і виявляють протиправні дії саме у ньому. У якості джерел інформації вони використовують журнали реєстрації подій (security log або syslog) для ОС,

МПЗ, СУБД й інших додатків. Інформація про події може бути отриманою хостовим сенсором також безпосередньо від мережевого екрану. Нині існують такі різновиди host-орієнтованих систем:

аналізатори реєстраційних файлів;

програми-wrappers – персональні міжмережеві екрани для окремих вузлів;

системи контроля цілісності тощо.

При цьому, наприклад, аналізатори реєстраційних файлів (Logfiles monitors, LFM), що розміщені на сервері безпеки здійснюють централізоване збирання та аналіз інформації, отриманої від хостових сенсорів. Як і мережеві сенсори вони шукають відомі сигнатури, але не у мережевому трафіку, а у файлах реєстрації, які вказують на те, що порушник здійснив атаку. Типовим прикладом LFM є синтаксичний аналізатор для log-файлів http-сервера WebStalker Pro. Його застосування дасть можливість ідентифікувати порушника, який намагається використати відомі уразливості та на основі аналізу реєстраційної інформації встановити факт: входу/виходу суб'єктів доступу до або з системи (вузла мережі); видачі друкованих (вихідних) документів; запуску/завершення програм і процесів (завдань, задач); зміни повноважень суб'єктів доступу; запуску програм суб'єктів доступу до файлів, що потребують захисту, включаючи їхнє створення, видалення, передачу по каналах зв'язку; доступу програм певних суб'єктів до вузлів мережі, каналів зв'язку, зовнішніх пристроїв комп'ютера, програм, каталогів, файлів, записів тощо. Зразками подібних програм є Intruder Alert компанії Symantec та RealSecure Server Sensor від Internet Security System.

Програми-wrappers для хостів конфігуруються таким чином, щоб на окремому комп'ютері контролювати всі мережеві пакети, спроби встановлення з'єднань з ним або входу на нього, а також спроби dial-in підключення (по телефону) або через інші немережеві порти зв'язку. Кращими зразками серед відомих пакетів даного типу є TC-wrappers для Unix систем і Outpost Network Security компанії Agnitum для Windows. Системи контролю цілісності (system integrity verifiers, SIV) перевіряють системні файли з метою встановлення факту й часу внесення в них змін. Такі системи використовують, як правило, криптографічні функції хешування. Кращими зразками серед них є програмні продукти типу Tripwire (http://tripwiresecuritv.com), L5 і SPI (http://ciac.llnl.gov) та ним подібні. Серед головних переваг хостових сенсорів слід відзначити їх можливість щодо ефективного виявлення внутрішніх і зовнішніх атак, які були пропущені мережевими сенсорами, а також констатації самих фактів їх здійснення. До недоліків слід віднести їх загостреність на роботу під керуванням певної ОС, перевантаженість системних ресурсів при детальному моніторингу, можливість проведення DDoS атаки при заповненні файлів результатів
аудиту, складність використання зібраної інформації тощо.

Засоби управління призначені для адміністрування усіх компонент системи виявлення атак та регулювання використовуваними інформаційними ресурсами. Їх основними функціями є:

ідентифікація користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);

аутентифікація (встановлення автентичності) об'єкта або суб'єкта після пред'явленого їм ідентифікатора;

перевірка повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);

надання дозволу і створення умов роботи в межах встановленого регламенту;

реєстрація (протоколювання) звернень до ресурсів, що захищаються;

реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Засоби реагування можуть бути розташованими на станціях моніторингу мережі,

між мережевому екрані, серверах та РСт ЛОМ. З метою негайного припинення атак ними перш за все оповіщається адміністратор безпеки (засобами електронної пошти, виведення повідомлень на консоль тощо), блокуються мережеві сесії та користувальницькі реєстраційні записи, заповнюється протокол дій атакуючої сторони тощо. При цьому рішення щодо вибору раціонального варіанта реагування на події безпеки приймається навіть за умови, якщо керуюча система не має достатньої інформації про стан інформаційного середовища. Процес вибору може бути описаний, згідно з [7], таким кортежем:

$$F_{АД}^{реагув} = \langle P_{АД}, P_{середовища}^{стан}, J, W_{реагув}^{раціон} \rangle , \quad (1)$$

де $P_{АД}$ – імовірність атакуючої дії (АД); $P_{середовища}^{стан}$ – імовірність стану середовища; J – цільова функція вибору; $W_{реагув}^{раціон}$ – раціональний варіант реагування.

Модель вибору раціонального варіанта реагування на події порушення безпеки серед, наприклад, можливих трьох (блокування в реальному часі доступу до Web-серверу з IP-адрес, що генерують потік HTTP-запитів; відбраковування будь-якого трафіку, вихідна адреса якого не є одною з IP-адрес певної установи та переконфігурування на маршрутизаторах і міжмережевих екранах функцій антиспуфінга та антиDoS) з урахуванням припустимого збитку від різних проявів стороннього кібернетичного впливу (за повної відсутності збитку; за наявності збитку, що зачіпає інтереси певного користувача або групи користувачів та за наявності збитку від реалізації кібератаки проти СІТС) може бути подана у вигляді орієнтованого графа (рис. 2) .

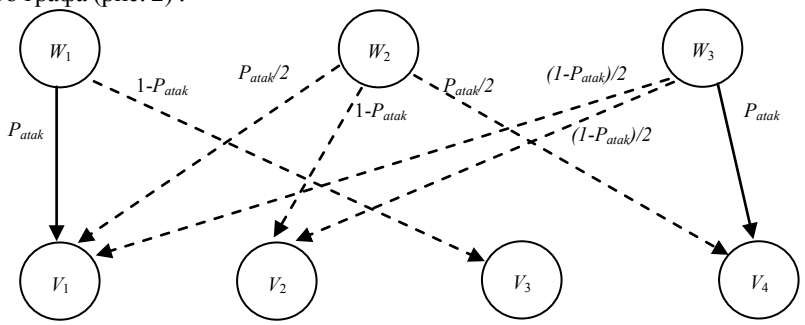

Рис. 2. Модель вибору раціонального варіанта реагування на події порушення безпеки

При цьому цільова функція вибору раціонального варіанту реагування на події порушення безпеки об'єктів захисту (табл. 1) задається згідно з [7–9] таким функціоналом:

$$J(W_i, z_l) = \sum_{l=1}^{s} C_j\left(V_j(W_i, z_l)\right) \cdot P_{середовища}^{стан}(z_l),\ i = \overline{1, N},\ j = \overline{1, L} \quad (2)$$

де $P_{середовища}^{стан}(z_l) = \prod_{i=1}^{I} p_{ij}$; $p_{ij} = p_{ij}\left(V_j(U_i), P_{АД}\right)$; $\forall i : \sum_j p_{ij} = 1$, p_{ij} – імовірність настання j-го збитку ($j = \overline{1,4}$) при виборі i-го ($i = \overline{1,3}$) варіанта реагування, W_i – варіант реагування на АД; V_j – результат реагування на W_i ; C_j – оцінка збитку від АД.

За таких обставин раціональний варіант реагування $W_{реагув}^{раціон}\left(P_{АД}\right)$ може бути визначений зокрема з виразу:

$$W_{реагув}^{раціон}(P_{АД}) = W\left(\min_i\left(J(W_i, z)\right)\right). \quad (3)$$

Таблиця 1

Об'єкти, що підлягають захисту, методи і засоби впливу на них та методи можливого реагування і протидії

Об'єкти	Засоби впливу, загроза	Можливі методи впливу	Методи реагування та протидії
Системи зв'язку: цифрові комутаційні системи; системи утворення каналів	Блокування роботи системи (вузла) управління, втручання в роботу системи (вузла) управління	Віддалене програмування системи (вузла) управління, занесення вірусів до ПЗ системи	Використання ліцензованого ПЗ, що має експертний висновок ДССЗЗІ, а також антивірусів
Канали зв'язку, канали передачі даних	Блокування каналів зв'язку та каналів передачі даних на транзитних вузлах	Втручання в роботу системи управління Центру управ- ління ВАТ "Укртелеком"	Блокування в реальному часі доступу до Web-серверу з IP адрес, що генерують потік HTTP запитів; відбраковування будь-якого трафіка, вихідна адреса якого не є одною з IP адрес; переконфігурування на марш рутизаторах і міжмережевих екранах функцій антиSpoofing і антиDoS тощо
Захищена система супутникового зв'язку	Блокування серверного обладнання та каналів супутникового зв'язку	Занесення вірусів до програмного забезпечення системи	Використання антивірусно-го ПЗ, блокування зовнішньо го підключення до системи
Канали супутникового зв'язку (СЗ)	Блокування каналів СЗ на транзитних вузлах	Втручання в роботу системи управління СЗ, занесення ві-русів до ПЗ системи, викори-стання передавачів завад	Резервування каналів, використання міжнародних кана-лів супутникового зв'язку
КХ радіоканали спеціального радіозв'язку	Завади роботі радіозв'язку	Використання передавачів завад	Резервування каналів
Сервери АС класу "3"	Блокування роботи сервера, спотворення інформації	Подолання системи захисту сервера та втручання в його роботу	Створення комплексної системи захисту інформації з підтвердженим атестатом
Сервери АС класу "2": ЛОМ	Блокування роботи сервера	Впровадження вірусних програм, програм шпигунів	
АРМ АС класу "3"	Блокування роботи АРМ, спотворення інформації, її перехоплення та підміна	Впровадження вірусних програм, програм шпигунів	
АРМ АС класу "2": ЛОМ, що обробляють ІзОД	Блокування роботи АРМ, НСД до інформації, витік інформації ТК, спотворен-ня інформації	Впровадження вірусних програм, програм шпигунів, порушення порядку роботи користувачами	
АРМ АС класу "1", що обробляють ІзОД	НСД до інформації, витік інформації ТК, спотворен-ня інформації	Впровадження вірусних програм, програм шпигунів, порушення порядку роботи користувачами	Створення комплексної системи захисту інформації з підтвердженим атестатом

Висновок. Дотримання основних вимог системи виявлення загроз безпеці інформації, що обробляється у СІТС дасть можливість:

понизити навантаження на персонал, що відповідає за інформаційну та кібербезпеку, а саме за виконання ним поточних операцій з контролю за користувачами (у тому числі й за тими, що мають адміністративні привілеї), а також за системами та мережами, що є компонентами СІТС;

ідентифікувати відомі атаки та інші прояви кіберзагроз й попереджати про них ві-

дповідальних за забезпечення інформаційної та кібербезпеки;

керувати засобами захисту та підвищити імовірність подолання загрози (табл. 2) за рахунок їх раціонального використання тощо.

Таблиця 2

Ймовірність подолання загрози певним засобом захисту
(дані отримані експертним методом оцінювання)

Вид атакуючої дії	Засіб захисту				
	Міжмережевий екран	VPN шлюз	Сервер обновлений	IDS	Антивірус
Троянські програми					0,96
Віруси					0,92
DoS-атаки	0,81	0,98		0,98	
DDoS-атаки	0,62	0,79		0,97	
Макровіруси					0,60
IP Spoofing	0,69	0,96		0,95	
DNS Spoofing				0,92	
WEB Spoofing				0,54	
Захоплення мережевих підключень	0,51	0,97		0,93	
Різні види сканування мережі	0,59			0,89	
Порушення конфіденційності даних		0,95	0,33		
Автоматичний підбір паролів	0,75			0,91	
Атаки на протоколи			0,52	0,79	
Неавторизоване використання прав	0,32			0,91	
Неконтрольоване використання ресурсів	0,53	0,61	0,32	0,81	0,64
Неавторизоване використання АС	0,62	0,73	0,29	0,79	0,67
Прослуховування мережі		0,92			
Злоякісне ПЗ: spyware, adware				0,54	0,97

При цьому нейтралізація загроз безпеки інформації у СІТС має здійснюватися виключно службами безпеки цих систем й забезпечуватись механізмами реалізації функцій цих служб. Вони у свою чергу повинні бути представлені відповідними, переважно програмно-технічними засобами – механізмами шифрування, цифрового підпису, контролю доступу, забезпечення цілісності даних, забезпечення аутентифікації, підстановки трафіку, керування маршрутизацією, арбітражу тощо. Отримані результати, як наслідок, можуть бути застосованими при створенні нових або удосконаленні існуючих механізмів злому систем захисту СІТС та визначенні множини відповідних показників, що характеризують безпеку комп'ютерних мереж на етапах проектування і експлуатації.

Література

1. Закон України "Про телекомунікації": за станом на 15.10.2011 р. / Затверджений ВР України, 18.11.2003, № 1280-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 24.12.2003, № 243.
2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": за станом на 30.04.2009 р. / Затверджений ВР України 05.07.1994, № 80/94-ВР. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 02.08.1994.
3. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.
4. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений, М: Юнити-Дана,

2001. – С. 261 – 278.
5. Закляков П. Обнаружение телекоммуникационных атак: теория и практика, Snort//Системный администратор. – 2003. – № 10(11).
6. Биячуев Т.А. Безопасность корпоративных сетей. / Т.А. Биячуев.; под ред. Л.Г. Осовецкого. – СПб: СПб ГУ ИТМО, 2004. – 161 с.
7. Машкина И.В. Управление и принятие решений в системах защиты информации : Учебн. пособие / И.В. Машкина. – Уфа: УГАТУ, 2007. – 160 с.
8. Котенко И.В. Анализ защищенности компьютерных сетей на основе модели-рования действий злоумышленников и построения графа атак. /И.В. Котенко, М.В. Степашкин. // Труды ИСА РАН. Т 31. – СПб., 2007. – С.126–207.
9. Анин Б.Ю. Защита компьютерной информации. / Б.Ю. Анин. – СПб.: БХВ-Петербург, 2000. – 384 с.

Надійшла до редколегії 05.05.2013 р.

Рецензент: д.т.н., проф. Петров А.С.

В.Л. Бурячок

СОВРЕМЕННЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ. МОДЕЛЬ ВЫБОРА РАЦИОНАЛЬНОГО ВАРИАНТА РЕАГИРОВАНИЯ НА ПРОЯВЛЕНИЯ ПОСТОРОННЕГО КИБЕРНЕТИЧЕСКОГО ВЛИЯНИЯ

В статье учитывая масштабы применения современных информационно-коммуникационных технологий и проблемы, связанные с обеспечением производительности, надежности и устойчивости функционирования информационно-телекоммуникационных систем, а также защиты от несанкционированного доступа циркулирующих в таких системах информационных ресурсов рассмотрен подход к формированию модели выбора рационального варианта реагирования на проявления постороннего кибернетического влияния.

Ключевые слова: IT системы, CITC, сеть, хост.

V.L. Buryachok

MODERN SYSTEMS OF INTRUSION DETECTION IN INFORMATION AND TELECOMMUNICATION SYSTEMS AND NETWORKS. THE SELECTION MODEL OF RATIONAL VARIANT OF RESPONDING TO THE OCCURRENCE OF EXTRANEOUS INFLUENCE CYBERNETIC

The article given the scale of the use of modern information and communication technologies and the problems associated with providing productivity, reliability and sustainability of information and telecommunication systems, as well as protection against unauthorized access to such systems, circulating information resources of the approach to the formation of a rational choice model of response options on display outside the cybernetic influence.Keywords: IT systems, SITS, the network host.

Keywords: IT systems, CITC, network, host.