УДК 003.26:004.7:053.072:519.876.5

Informatics and Mathematical Methods in Simulation
Vol. 7 (2017), No. 3, pp. 205-212

ДИНАМІЧНІ ВЛАСТИВОСТІ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА ПРИКЛАДІ АУДИТУ КІБЕРБЕЗПЕКИ

О.Ю. Козлова[1], В.Г.Кононович[1], І.В. Кононович[2], М.Г. Романюков[1], Л.М. Тимошенко[1]

[1] Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net
[2] Одеська національна академія харчових технологій
вул. Канатна, 112, м. Одеса, 65039, Україна; e-mail: kononovich@mail.ru

У роботі розглянуто процес розвитку від інформаційної безпеки до кібернетичної безпеки об'єктів інфраструктури, і зокрема процесів аудиту кіберзахищеності. Встановлено, що аспекти динаміки процесів інформаційної та кібербезпеки досліджені недостатньо, і не розкривають повний формальний та системний підхід до вирішення задач кібербезпеки. У зв'язку з цим, розроблена логіко-лінгвістична модель ризико-орієнтованого підходу до планування заходів кібербезпеки та найпростіша математична модель двох етапного циклічного управління процесами аудиту. Використання математичної моделі буде сприяти більш точному розумінню динамічних властивостей та розробці необхідних системних і позасистемних заходів забезпечення кібербезпеки.

Ключові слова: кібернетична безпека, модель динамічної системи, циклічне управління аудитом.

Вступ

Інформаційний та кібернетичний простори відіграють важливу роль в економічному та соціальному розвитку кожної країни світу. В Україні існує ціла низка проблем вразливості інформаційної сфери відносно стороннього кібернетичного впливу. Протистояти фізичному руйнуванню технічних засобів, порушенню функціонування об'єктів нападу та протиправній діяльності соціальних інженерів з дня на день стає все важче через недостатнє кадрове забезпечення відповідними фахівцями у сфері інформаційної та кібербезпеки. Необхідним є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1].

Небезпека кіберзлочинності була усвідомлена ще в часи приєднання України до міжнародної «Конвенції про кіберзлочинність». А термін «кібербезпека кіберпростору» з'явився у лексиконі українських спеціалістів зовсім недавно. І, перш за все, спалахнула термінологічна суперечка. Визначення понять «інформаційна безпека» та «кібербезпека» дуже схожі у багатьох авторів [1–3] і формально відрізняються додаванням понять «кіберпростір», як об'єкту захисту, «кіберзагроз» тощо. Кібербезпека розглядається як безпека специфічного виду інформації – управлінської інформації [2]. Приставка «кібер-» виділяє «клас кіберсистем, які використовуються для вирішення задач управлінського характеру». «В кіберсистемах на перше місце виділяється вимоги неперервності й стійкості управління. А ці вимоги можуть бути виконані лише при умові забезпечення доступності, цілісності та конфіденційності вхідної інформації [3]». Для остаточного розуміння цих термінів ще потрібні додаткові дослідження.

Міжнародна спільнота накопичила немалу кількість стандартів та передових практик захисту найважливіших об'єктів інфраструктури [4]. Важливе місце в системі як інформаційної безпеки, так і кібербезпеки займає аудит [5, 6]. Основним призначенням *аудиту* інформаційної безпеки об'єкта інформаційної діяльності є формування, як правило, незалежної оцінки інформаційної безпеки.

За метою проведення аудит поділяється на аудит для підтвердження відповідності вимогам національної системи нормативно-правових документів інформаційної безпеки та на аудит підтвердження відповідності міжнародним стандартам ISO\IEC 15408 [7]».

Як і в багатьох сферах при системному підході системи інформаційної безпеки розглядаються як динамічні системи, які складаються із множини механізмів і функцій, які теоретики пов'язують із феноменом самоорганізації. Ряд спеціалістів застосовують методи нелінійної динаміки для вивчення властивостей процесів захисту інформації [8,9]. Процеси аудиту, зокрема внутрішнього, є принципово циклічним і нелінійними. Ці питання потребують своєї розробки.

Метою роботи є удосконалення термінології у частині понять «кібербезпеки» та розроблення найпростішої дискретної математичної моделі динаміки циклічного процесу обробки даних аудиту.

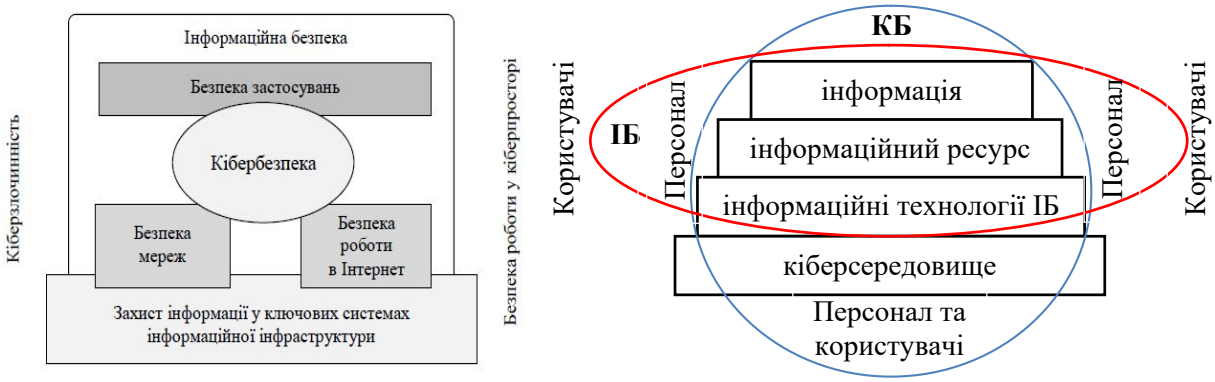
Визначення кібербезпеки та інформаційної безпеки

Закон України про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 року визначає «кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенціальних загроз національній безпеці України у кіберпросторі», де «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікації з використанням мережі Інтернет та або інших глобальних мереж передачі даних». «Кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [10]». В чинному документі Закону України про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки від 9 січня 2007 року визначається «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [11]».

Взаємовідношення понять у сферах безпеки в кіберпросторі у контексті ISO 27032 представлені на рис. 1. Кібербезпека забезпечується у наступних сферах: безпека застосувань і операційних систем, безпека інформаційно-комунікаційних мереж, безпека роботи в Інтернет, захист інформації у ключових системах інформаційної інфраструктури і, зокрема, в об'єктах критичної інфраструктури, а також у сферах боротьби з кіберзлочинністю та забезпечення безпеки роботи у кіберпросторі. Даний рисунок справляє те уявлення, що кібербезпека є складовою частиною інформаційної безпеки. Формально це так. Кібернетичні системи, як системи управління, у своєму

сучасному вигляді, являються підмножиною інформаційних систем. Поняття кібербезпеки прийшло із військової сфери, де офіційно було застосоване в управлінні.

Але, судячи з визначень, які наведено вище, поняття «кібербезпека» більш ширше у відношенні об'єктів, яких воно стосується. На рис. 1 показані об'єкти/суб'єкти які охоплюються, відповідно, інформаційною (ІБ) та кібернетичною безпекою (КБ).



а б

Рис. 1. Взаємовідношення понять у сферах безпеки в кіберпросторі: а – місце кібербезпеки серед інших сфер безпеки (Джерело – ISO 27032:2012); б – охоплення об'єктів інформаційної та кібербезпеки

Ретроспективно системи захисту інформації розвивалось наступними етапами:

– захист інформації системами технічного та криптографічного захисту, за допомогою криптографічних, технічних, організаційних, а тепер і програмних засобів;

– забезпечення інформаційної безпеки інформаційних ресурсів в автоматизованих системах. До інформаційних ресурсів відноситься інформація, засоби обробки інформації та (звернемо увагу) обслуговуючий персонал (НД ТЗІ 1.1-003-99);

– забезпечення інформаційної безпеки інформаційних технологій, зокрема в інформаційно-комунікаційних системах. На цьому етапі об'єктом захисту стає також відкрита інформація, важлива для особи, суспільства та держави;

– забезпечення кібернетичної безпеки кіберпростору. Кіберпростір охоплює інформацію, інформаційні технології, персонал, користувачів і все те, що виникає при комунікаціях суб'єктів і об'єктів та взаємодії їх між собою.

Сформулюємо головні відмінності інформаційної та кібербезпеки, користуючись переліком «Базові заходи кібербезпеки», які наведені у [12]:

– Об'єктом забезпечення кібербезпеки стає кіберпростір. Його важлива складова – інформаційно-комунікаційна та телекомунікаційна системи.

– Ще більше приділяється уваги готовності мереж, що важливо з точки зору відбиття DDOS-атак.

– Суб'єктом забезпечення кібербезпеки стають, крім персоналу, конечні користувачі, Для безпеки конечних користувачів передбачаються низка заходів, включаючи застосування персональних між мережевих екранів та систем виявлення вторгнень.

– Методи соціальної інженерії є не лише засобом нападу, а й захистом від атак.

– Актуалізуються як обов'язкові процеси менеджменту, моніторингу і аудиту, динаміка яких є предметом даного дослідження.

Управління процесами аудиту інформаційної безпеки

Управлінський цикл – це сукупність послідовно здійснюваних управлінських

операцій, у ході яких суб'єкт управління досягає бажаних результатів. У кожному циклі спостерігається певна послідовність управлінських дій. Додержання певного порядку їх виконання має важливе значення для забезпечення високої якості управління.

Прогнозування – це метод, в якому використовується як накопичений в минулому досвід, так і поточні припущення стосовно майбутнього з ціллю його визначення. Якщо прогнозування виконано якісно, результатом стане картина майбутнього, яку можна використовувати як основу для планування.

Циклічність і прогнозування за допомогою попередніх циклів майбутніх станів складають суть сучасного підходу до процесно-орієнтованого управління, тобто ідентифікації процесів та управління ними

Для зниження відхилень в управлінні можна застосувати концепцію PDCA (рис. 2). Основними елементами циклу являються:

P – визначення цілей та прийняття рішення щодо необхідних змін, тобто розробка плану;

D – здійснення змін або втілення плану;

C – контроль виконання плану;

A – проведення необхідних дій, якщо результати не відповідають запланованим, або стандартизація в іншому випадку.

Рис. 2. Цикл постійного поліпшення системи менеджменту якості

При управлінні інформаційною безпекою використовують процеси оцінки ризиків інформаційної безпеки, організації і експлуатації захисних заходів, навчання персоналу інформаційній безпеці та інші. Серед них визначальними є процеси контролю та перевірки інформаційної безпеки. Аудит займає особливе місце в системі забезпечення інформаційної безпеки об'єкта інформаційної діяльності, який формує незалежну оцінку інформаційної безпеки. Своєчасність, точність і повнота оцінок інформаційної безпеки, отриманих у результаті аудиту, дають змогу виявити вразливості системи, скоригувати їх, щоб удосконалити процеси забезпечення інформаційної безпеки.

Результативність, надійність та об'єктивність висновків за результатами аудиту забезпечуються чітким дотриманням принципів проведення аудиту, таких як: відповідальність, обачність, неупередженість, непідкупність та уміння зберігати таємницю та інших.

Використання ризико-орієнтованого підходу до планування заходів аудиту є одним з можливих варіантів збільшення ефективності аудиту (рис. 3).

Аудит може бути зовнішнім та внутрішнім за методами проведення.

Зовнішній аудит – разовий захід та проводиться за ініціативою керівництва сторонньою організацією відповідної кваліфікації. Висновки за результатами цього

аудиту використовуються для покращення якості процесів організації. Проводити його слід регулярно.

Для самооцінки стану інформаційної безпеки силами самої організації проводиться внутрішній аудит, тобто проводиться пошук слабких місць, покращення якості процесів організації, оцінка ступеня відповідності системи забезпечення безпеки вимогам діючих нормативно-правових документів. Ця діяльність є безперервною і затверджується керівництвом організації.

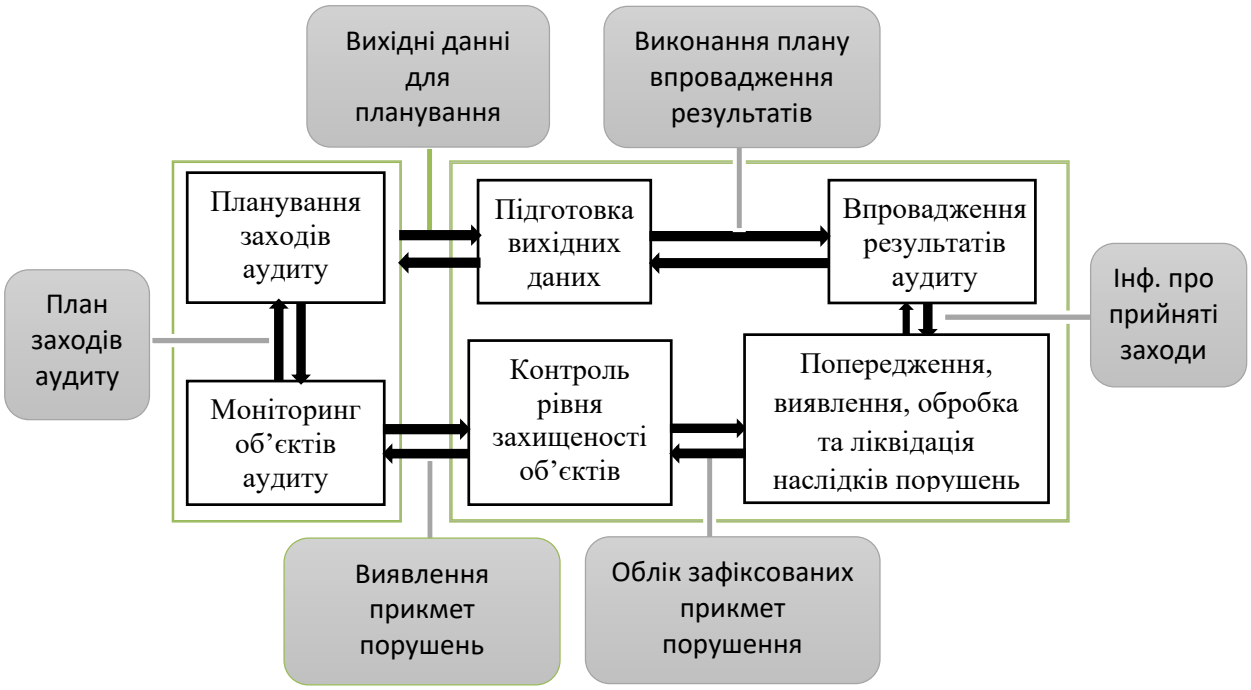


Рис. 3. Схема реалізації ризико-орієнтованого підходу до планування заходів аудиту

Аудит починається з процедури ініціації. На цьому етапі повинні бути визначені межі проведення обстеження, до яких відносяться переліки: фізичних осіб, ресурсів, приміщення, основні види загроз, організаційні, фізичні та програмно-технічні аспекти забезпечення інформаційної безпеки.

Найскладніший та найтриваліший етап збирання інформації аудиту, тому що саме на цьому етапі проводиться вивчення документації та тісна взаємодія аудитора з посадовими особами організації.

Далі аудитори повинні виконати аналіз даних, при цьому можна використовувати один із трьох методів.

Перший підхід, який базується на аналізі ризиків – найскладніший, трудомісткий та вимагає найвищої кваліфікації аудитора, тому що необхідно визначити індивідуальний набір вимог інформаційної безпеки, що враховує особливості середовища її функціонування та існуючі загрози інформаційної безпеки.

Другий підхід – практичний та опирається на використання стандартів інформаційної безпеки, які визначають базовий набір вимог інформаційної безпеки. Стандарти можуть визначити різні набори вимог залежно від рівня захищеності, приналежності та призначення.

Третій підхід припускає комбінування перших двох. Він є найефективніший. Базовий набір вимог інформаційної безпеки визначається стандартом, додаткові вимоги формуються а основі аналізу ризиків.

Четвертий підхід складний і найбільш відповідальний. Аналіз ризиків – це те, з чого повинна починатися побудова будь-якої інформаційної безпеки. Він полягає у виявленні існуючих ризиків та їх оцінки якісної або кількісної.

Далі проводиться оцінка відповідності вимогам стандартів. Виявляться вимоги інформаційної безпеки, які не реалізовані в системі. Виходячи з цього, робляться висновки про відповідність.

Вироблення рекомендацій за наслідками аналізу, які повинні бути конкретними, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізи) і відсортованими за ступенем важливості.

Підготовка звітних документів, які повинні містити опис цілей проведення аудиту, характеристику обстеження, вказівку границь проведення аудиту та методів. Звіт є основним результатом проведення аудиту, якість якого характеризує якісь роботи аудитора.

Математична модель циклічного управління процесами аудиту

Подібна задача вирішувалась авторами, стосовно циклічного управління кібербезпекою в [8] і стосовно управління колективною та індивідуальною свідомістю громадян у [9]. «Ефективність людської дії здебільшого залежить від правильного управлінського рішення, що, у свою чергу, залежить від інформаційного моделювання ситуації, від пошуку потрібної інформації та її переробки. Лавиноподібне зростання інформаційних потоків, у яких змішувались потрібна і непотрібна інформація («інформаційні шуми»), у значній мірі утруднив поведінку людини та висунув на передній план вибірковий пошук потрібної інформації з наступною її редукцією для прийняття тих чи інших рішень [13]».

Розглянемо найпростішу модель циклового інформаційного процесу управління, який складається з двох етапів:

- аналізу інформаційного потоку даних аудиту (відбір потрібної інформації, редукція, консолідація, переробка) – x_{in};

- прийняття рішень та обробки вихідного інформаційного потоку для корекції заходів захисту (формування та видача управлінського рішення) – x_{out}.

Математична модель динамічної системи $\Phi(x, y)$ буде мати такий вигляд:

$$\Phi(x,y)=\begin{cases} x_{n+1} = x_n - k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in} \\ \\ y_{n+1} = y_n + k_{xy} p x_n^2 - (k_{yx} + k_{out}) q y_n^2 \end{cases} \quad (1)$$

де x, y – динамічні змінні, які визначають інтенсивність інформаційних елементів потоку на етапах обробки інформації; k_{ij} – перехідні коефіцієнти, що характеризують динамічну взаємодію етапів обробки інформації; p, q – розподільчі коефіцієнти, x_{in} – інтенсивність інформаційних елементів потоку, що поступають на перший етап обробки; причому, $\{k_{ij}\}$ и $\{p, q\} \in (0,1)$, $\{x, y\} \in R$, $x_{in} = const \in R^+$.

Наявність у системі двох груп коефіцієнтів (k_{ij} та p, q) має конкретну фізичну інтерпретацію: коефіцієнти k_{ij} описують відносну величину редукції і консолідації інформації за синтаксичними ознаками, наприклад, форматами відомостей і повідомлень, та задають долю інформаційного потоку, який переходить з одного етапу на сусідній. Частина інформаційного потоку переходить на попередній етап обробки для виправлення неточностей, врахування зауважень тощо. Коефіцієнти p, q описують розподіл елементів інформаційного потоку за їх видами по семантичним ознакам, наприклад, по змісту. Перехід між етапами обробки визначається добутком коефіцієнтів обох груп.

Висновки

Уточнення понять, пов'язаних з поняттям «кібербезпека» здійснено відносно розширення об'єктів забезпечення кібербезпеки у порівнянні з інформаційною безпекою, та визначення нових суб'єктів та механізмів кібербезпеки. Розроблена найпростіша дискретна математична модель динаміки циклічного процесу обробки даних аудиту, яка описує два етапи: етап аналізу інформаційного потоку даних аудиту (відбір потрібної інформації, редукція, консолідація, переробка); та етап прийняття рішень й обробки вихідного інформаційного потоку для корекції заходів захисту (формування та видача управлінського рішення). Напрямом подальшої роботи буде детальний аналіз моделі динаміки процесів аудиту кібербезпеки.

Список літератури

1. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
2. Соколов, М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право, 2012. – № 1. – 24 с.
3. Архипов, А. Приставка кибер-: все ли очевидно? / Александр Архипов // Захист інформації, 2016. – Том 18, №3. – С. 203-209.
4. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства / Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам Секретариата ОБСЕ. – ОБСЕ: Vienna, Austria, 2013. – 96 с.
5. Курило, А.П. Аудит информационной безопасности / Курило А.П., Зефиров С.Л., Голованов В.Б. / М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
6. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / Корченко О.Г., Гнатюк С.О., Казмірчук С.В.– К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с. .
7. Тардаскіна, Т.М., Кононович В.Г. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посібник. Затверджено Міністерством освіти та науки України як навчальний посібник для студентів вищих навчальних закладів [Лист № 1/11-7791 від 13 серпня 2010 року] / – Одеса: ОНАЗ, 2010. – 268 с.
8. Кононович, В.Г. Нелінійні моделі циклічного управління кібербезпекою / В.Г. Кононович, І.В. Кононович, А.І. Міхова // «Інформаційні управляючі системи та технології» (ІУСТ – ОДЕСА – 2015). Матеріали Міжнародної науково-практичної конференції, 22 – 24 вересня 2015., Одеса / відп. ред. В.В. Вичужанін, 2015.– С.171 – 173.
9. Кононович, В.Г. Модель системы информационной безопасности консолидированной информации при информационном противоборстве (Раздел 16) / В.Г. Кононович, И.В. Кононович // Информационные технологии и защита информации в информационно-коммуникационных системах : монография / под редакцией В.С. Пономаренко – Х. : Вид-во ТОВ «Щедра садиба плюс», 2015.– С. 220 – 233.
10. Законодавство України: Наказ від 05.10.2017 № 2163-19 [Електронний ресурс] // Про Основні засади забезпечення кібербезпеки України. Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.10.2017).
11. Законодавство України: Наказ від 09.01.2007 № 537-16 [Електронний ресурс] // Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Режим доступу: http://zakon0.rada.gov.ua/laws/show/537-16 (дата звернення: 10.10.2017).
12. Марков, А.С. Руководящие указания по кибербезопасности в контексте ISO 27032 / А.С. Марков, В.Л. Цирлов // Вопросы Кибербезопасности, 2014. – № 1(2). – С. 28-25.
13. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; Ин-т проблем передачи информ. РАН. – М.: Наука, 2006. – Т.1 – 495 с.

ДИНАМИЧЕСКИЕ СВОЙСТВА ПРОЦЕССОВ ОБЕСПЕЧЕНИНЯ КИБЕРБЕЗОПАСНОСТИ НА ПРИМЕРЕ АУДИТА КИБЕРБЕЗОПАСНОСТИ

О.Ю. Козлова[1], В.Г. Кононович[1], І.В. Кононович[2], М.Г. Романюков[1], Л.М. Тимошенко[1]

[1]Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net
[2]Одесская национальная академия пищевых технологий
ул. Канатная, 112, м. Одесса, 65039, Украина; e-mail: kononovich@mail.ru

В работе рассмотрено процесс развития от информационной безопасности до кибернетической безопасности объектов инфраструктуры, и в частности, процессов аудита кибернетической защищенности. Установлено, что аспекты динамики процессов информационной и кибербезопасности исследованы недостаточно. и не раскрывают полный формальный и системный подход к решению задач кибербезопасности. В связи с этим, разработана логико-лингвистическая модель риск-ориентированного подхода к планированию мероприятий кибербезопасности и наипростейшая математическая модель двухэтапного циклического управления процессами аудита. Использование математической модели будет способствовать более точному пониманию динамических свойств и разработке необходимых системных и внесистемных мероприятий обеспечения кибербезопасности.
Ключевые слова: кибернетическая безопасность, модель динамической системы, циклическое управление аудитом.

DYNAMIC PROPERTIES OF PROVIDING OF CYBERSECURITY ON THE EXAMPLE OF CYBERSECURITY AUDIT

O.Yu. Kozlova[1], V.G. Kononovich [1], I.V. Kononovich [2], M.G, Romanukov[1], L.M. Timoshenko[1]

[1] Odessa National Polytechnic University,
1, Shevchenko Ave, Odessa, 65044, Ukraine; e-mail: vl_kononovich@ukr.net
[2] Odessa National Academy of Food Technologies
112, Kanatna Str, Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

The paper considers the process of development from information security to cybernetic security of infrastructure objects, in particular, the processes of cyber security audit. It has been established that the aspects of the dynamics of information and cyber security processes have not been adequately studied. and do not disclose the full formal and systematic approach to solving cyber security problems. In this regard, developed a logical-linguistic model of a risk-oriented approach to planning cyber security activities and the simplest mathematical model of two-stage cyclical management of audit processes. The use of the mathematical model will contribute to a more accurate understanding of the dynamic properties and the development of the necessary system and non-systemic measures to ensure cybersecurity.
Keywords: cybernetic security, model of dynamic system, cybersecurity audit.