© Kononovich V., Staikutsa S., Kononovich I., Kopytin Yu., Romanyukov N. Adaptive approaches to cybersecurity of distributed and hierarchical management systems // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 3, p. 255-260.

DOI: 10.18372/2225-5036.22.11101

АДАПТИВНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ РОЗПОДІЛЕНИХ ТА ІЄРАРХІЧНИХ СИСТЕМ УПРАВЛІННЯ

Володимир Кононович[1], Сергій Стайкуца[2], Ірина Кононович[3], Юрій Копитін[4], Микола Романюков[5]

[1]Одеський національний політехнічний університет, Україна
[2]Одеська національна академія зв'язку ім. О.С.Попова, Україна
[3]Одеська національна академія харчових технологій, Україна
[4]КП «Обласний інформаційно-аналітичний центр», м. Одеса, Україна
[5]Головне управління Національної поліції в Одеській обл., Україна

КОНОНОВИЧ Володимир Григорович, к.т.н.

Рік та місце народження: 1941 рік, с. Баришівка, Київської обл., Україна.
Освіта: Одеський електротехнічний інститут зв'язку, 1968 рік.
Посада: доцент кафедри інформаційної безпеки та передачі даних з 2010 року.
Наукові інтереси: теорія інформації, неокібернетика та кібербезпека.
Публікації: більше 200 наукових публікацій, навчальні посібники та авторські свідоцтва.
E-mail: kononovich@mail.ru

СТАЙКУЦА Сергій Володимирович, к.ф.н.

Рік та місце народження: 1978 рік, м. Вознесенськ, Миколаївської обл., Україна.
Освіта: Одеська національна академія зв'язку, 2001 рік.
Посада: доцент кафедри інформаційної безпеки та передачі даних з 2010 року.
Наукові інтереси: соціальна філософія, інформаційна безпека, системи захисту бізнесу.
Публікації: 18 наукових робіт, серед яких монографія, навчальні посібники, наукові статті та доповіді на міжнародних конференціях та семінарах.
E-mail: s.staikuca@gmail.com

КОНОНОВИЧ Ірина Володимирівна

Рік та місце народження: 1979 рік, м. Одеса, Україна.
Освіта: Одеська державна академія холоду, 2001 рік.
Посада: викладач кафедри інформаційних технологій та кібербезпеки Одеської національної академії харчових технологій з 2002 року.
Наукові інтереси: теорія інформаційного виробництва, інформаційна безпека.
Публікації: 27 наукових статей та доповідей на міжнародних конференціях та семінарах.
E-mail: kononovich@mail.ru

КОПИТІН Юрій Вікторович

Рік та місце народження: 1989 рік, м. Одеса, Україна.
Освіта: Одеська національна академія зв'язку, 2011 рік.
Посада: т.в.о. начальника відділу забезпечення захисту інформації КП «Обласний інформаційно-аналітичний центр» з 2013 року. Аспірант ОНАЗ
Наукові інтереси: управління інформаційною безпекою, економічна безпека.
Публікації: 16 наукових статей та доповідей на міжнародних конференціях та семінарах, навчальний посібник.
E-mail: ykopytin@odessa.gov.ua

РОМАНЮКОВ Микола Генріхович

Рік та місце народження: 1987 рік, м. Мала Виска, Кіровоградської обл., Україна.
Освіта: Харківський національний університет внутрішніх справ, 2010 рік.
Посада: старший інспектор управління режиму та технічного захисту інформації Головного управління Національної поліції в Одеській області
Наукові інтереси: управління інформаційною безпекою, технічний захист інформації.
Публікації: 9 наукових статей та доповідей на міжнародних конференціях та семінарах.
E-mail: kolyanr21@gmail.com

Анотація. *Проблема кібербезпеки в умовах деструктивних інформаційних впливів являється однією з гострих проблем у сучасному і майбутньому суспільствах високих технологій. Системи управління, як і інформаційні технології, стали надскладними й інтенсивно автоматизуються. У галузі державного управління та управління інформаційним виробництвом рівень критичності підсилюється підвищеним обсягом інформації, яку необхідно обробляти, розподіленими інтенсивними комунікаціями, ієрархічністю систем та появою нових уразливостей і потенційних загроз. Існуючі наукові і практичні роботи не в повній мірі враховують сучасні вимоги нормативно-керівних документів щодо безпеки розподілених та ієрархічних систем управління, не дають можливості враховувати для аналізу та оцінки безпеки управління поведінкою вибору та потреб безпеки суспільства, породженою новою матеріальною технологію у суспільстві високих технологій. Виходячи з цього, на базі історичного аналізу трансформації основних підходів до захисту інформації, яка використовується для управління, запропоновано адаптивний підхід до побудови ієрархічної чотириступеневої системи кібербезпеки: від забезпечення безпеки інформаційних пакетів і відомостей до забезпечення безпеки матриць цінностей та картин бачення світу. У подальших роботах заплановано розробку методів реалізації сформованих у цій роботі підходів.*

Ключові слова: *кібербезпека, інформаційна безпека, загрози, суспільство високих технологій, інформаційний вплив, матриці цінності, картини бачення світу.*

Вступ

За останні 20 років відбулись глибокі зміни в економіці, суспільстві, праві, інформаційних і суспільних технологіях. Напрями, причини, умови, технології та наслідки подальшого розвитку інформаційної революції проаналізовано в [1] на основі стратегій і планів транснаціональної компанії IBM – як дзеркала змін.

Ми живемо у перехідний період до інформаційного суспільства та суспільства високих технологій. Інформаційні технології (ІТ) вийшли на промисловий рівень, інформація придбала нові функції: засобу виробництва, сировини інформаційного виробництва, продукту та товару. Структурні зміни перетворюють фінансово-економічні сфери, структури влади і навіть соціальний устрій суспільства та соціальні інститути. Змінюються образ життя особистості і суспільства, їх світогляд.

«На перший план виходить розвиток та еволюція соціуму з його інтелектуальними, творчими, морально-етичними активами і цінностями. … Парадигма сучасної соціальної реальності сильно змінилась. Глобальна дигітилізація та інформатизація торкнулась практично усіх видів діяльності суспільства, і в першу чергу, військової сфери. Сильно змінилась швидкість доставки інформації, створені системи миттєвого інформаційного реагування і контролю [1]».

Очевидно, що засоби управління інформацією та дезінформацією являються потужною інформаційною зброєю. Як писала «The Times» 10 серпня 2016 року «Планету жде «зміна парадигм», настільки ж радикальна, як заміна кавалерії на танки, ситуація, коли на війні «зброєю стає що завгодно»». Газета перелічує: «застосування дезінформації для зриву демократичних дебатів, кібератаки, економічна політика з метою тиску; розгортання не декларованих військ, які стають поштовхом до більш стандартного військового втручання [2]».

«Проблеми інформаційної безпеки вийшли на новий рівень. Постала необхідність захисту інформаційних просторів, активів, каналів, грошей (електронних), фінансових потоків, інформації, що несе знання та забезпечує управління, інформаційні мережі, які об'єднують джерела інформації, команди компетентних спеціалістів і канали комунікацій. Практично всі сучасні ІТ-платформи виявились пронизаними технологічними засобами шпигунського контролю й моніторингу. Контур стратегічного управління вимагає надійної системи безпеки та спеціального захисту від зовнішнього агресора, тому що це самий вразливий актив, як і розум людини [1, с. 93]».

Зміни структури активів та поява нематеріальних цінностей створюють нові загрози і вразливості. Потрібні нові адекватні рішення й технології захисту. Треба «захистити свої активи при нестатку кваліфікованих кадрів і росту витрат на захист даних [1, с. 97]». Виникає проблема: як глобальні зміни впливають на трансформацію сфери інформаційної безпеки та кібербезпеки.

Аналіз існуючих досліджень

Сфера кібербезпеки стала інтенсивно розвиватись з часу гібридної війни проти України і, особливо з прийняттям «Стратегії кібербезпеки України» [3]. Нормативно-правова база знаходиться у стадії створення. Серед робіт, пов'язаних із забезпеченням кібербезпеки варто виділити роботу В. Харченка, О. Корченка та С. Гнатюка, наприклад, [4], які розглядають підвищення безпеки інформаційно-комунікаційного середовища транспорту.

Ніяка влада не може існувати без таємниць і секретів. При цьому, «масове розповсюдження та доступність ІТ вже створили, на перший погляд, абсурдну ситуацію, за якої практично будь-який бажаючий з мінімальними витратами може отримати повний обсяг інформації, необхідний для прийняття правильних управлінських рішень [5]».

З іншого боку, можливості розвідок, особливо технічних, значно зросли. З'явилось таке явище, як «великі дані». Статистика кіберзлочинів і порушень інформаційної безпеки невтішна. «У гіпербібліотеках накопичуються гігантські об'єми даних. А у співставленні між собою вони дозволяють отримати більше 99% відомостей, які потрібні для управління конкурентною боротьбою у бізнесі або боротьбою за владу у політиці [5]».

У сьогоденні розвиваються ідеї адаптивного підходу до проблем безпеки. Варто виділити розробки адаптивного підходу до забезпечення безпеки розподілених комп'ютерних систем (РКС) В. Мухіна та Г. Луцького на основі «інтеграції у захищену систему налаштованих засобів контролю доступу, засобів забезпечення цілісності даних та засобів управління конфігурацією програмного забезпечення розподілених систем із врахуванням потрібного рівня захищеності РКС [6]».

Розроблений адаптивний підхід засновується на максимальній уніфікації всіх взаємодій у системі. Серед зарубіжних матеріалів щодо адаптивної архітектури безпеки варто ознайомитись з [7], які свідчать про вихід цієї проблеми до практичного вирішення.

Важливий вклад в питання оцінки шкоди національній безпеці України у разі витоку державної таємниці внесла монографія [8].

Проте більшість відомих робіт розглядає загальні підходи до забезпечення кібербезпеки інформації, що зберігається, обробляється і передається за допомогою сучасних РКС. Таким чином, сучасні наукові дослідження не в повній мірі враховують сучасні підходи до забезпечення кібербезпеки ієрархічних розподілених інформаційно-комунікаційних систем. Своєчасність і актуальність тематик такого роду досліджень не сумнівна.

Мета роботи. Розробка адаптивного підходу до побудови ієрархічної чотириступеневої системи кібербезпеки систем державного й суспільного управління, з врахуванням можливих ознак та властивостей майбутнього суспільства високих технологій.

Основна частина дослідження

Складність, мінливість внаслідок свого прискореного розвитку та масове розповсюдження ІТ знижує ефективність забезпечення кібербезпеки, вносячи нові вразливості та загрози. У той же час, створюються нові широкі можливості для розвідки. Об'єкти захисту – системи державного, суспільного та виробничого управління – стають складними, розподіленими та ієрархічними. Зміни підходів до забезпечення безпеки слідують (адаптуються) за змінами того, якого виду інформація використовується в інтересах управління, а останні залежать від трансформацій суспільного устрою та способів управління. Приведемо докази необхідності адаптивного підходу до системи кібербезпеки ієрархічних систем.

«Влада не може існувати без таємниці [5]». В суспільстві існує бар'єр між правлячим класом і громадськістю, між державним управлінням і горизонтальними суспільними відносинами людей чи спільнот. Раніше це були класові та станові бар'єри, тепер – бар'єри організованої доступності.

А. Денисов до основної технології влади, яка вимагає захисту, відносить технології управління поведінкою вибору. «Саме у цьому і полягає влада – управляти вибором, які здійснюють люди [10]». Логіка трансформацій цього вибору в різні історичні епохи впливає на трансформацію принципів і цілей засекречування та захисту інформації. За цією характеристикою доцільно розглянути чотири історичні епохи, в яких перехід до нового етапу технологічної розвитку приводив до виникнення нового правлячого класу та технологій управління:

Розглянемо трансформації технологій управління поведінкою вибору і, пов'язаних з ними об'єктами, принципами та цілями засекречування й забезпечення кібербезпеки.

Трансформації технологій управління поведінкою вибору:

– епоха 1, феодальне або кріпосне (доіндустріальне) суспільство. Управління в умовах примусової ручної праці, відсутність вибору (непокірні знищуються). Це управління, по А. Денисову, за *змістом* міжособистісних комунікацій (що думають і що роблять);

– епоха 2, індустріальне буржуазне (або соціалістичне) суспільство. Управління за моделлю «стимул-реакція» в умовах вільного продажу праці на ринку праці, важка фізична праця механізується, а на просунутому етапі автоматизується, непокірні залишаються без засобів існування, або позбавляються волі. Це управління, по А. Денисову, за *характером* міжособистісних комунікацій (як спілкуються і як роблять). За сучасними теоріями – це управління за принципом зворотного зв'язку (регулятор Уатта). Нині – це кібернетика 1-го порядку;

– епоха 3, постіндустріальне, перехідне доінформаційного суспільства, (інвестиційна фаза). Рефлексивне управління за моделлю рефлексії свідомості в умовах свободи і дотримання прав людини й вільного індивідуального вибору в навколишньому середовищі, до якого додається «віртуальна» реальність; важка, небезпечна для здоров'я та одноманітна праця роботизується, на просунутому етапі автоматизується розумова праця, зароджується технократичний спосіб мислення та мережевий колективний розум [1, с. 91], нездатні і незгодні працювати переводяться на соціальне утримання, або позбавляються волі. Це управління з використовуванням, по А. Денисову, концепції лише єдиної індивідуальної свідомості; За сучасними теоріями – це рефлексивне управління за принципом кібернетики 2-го порядку та наступних, які описують системи із самосвідомістю. «Його неможливо освоїти, не отримавши хоро-

шого базового інженерного або фізико-математичної освіти [5]»;.

– епоха 4, суспільство високих технологій, винайдених у інноваційній фазі. Рефлексивне управління поведінкою вибору за моделлю рефлексії свідомості з використовуванням, по А. Денисову, концепції множинності шарів індивідуальної свідомості. Епоха характеризується як назріваюча інтелектуально-гуманітарна революція [1, с. 94].

Таким чином, технології управління поведінкою вибору визначають, по А. Денисову, наступні предмети і засоби управління за епохами:

1. Управління *змістом* міжособистісного інформаційного обміну за допомогою *сили*.

2. Управління каналами, характером і трафіком міжособистісного інформаційного обміну за допомогою законодавчих, організаційних, технічних, програмних, а особливо останнього часу, й соціально-психологічних засобів. Прикладом такого управління, яке включає в себе й управління інформаційною безпекою може бути робота [9].

3. Рефлексивне управління *усвідомленням поведінки вибору*, заснованому на математичних моделях морального вибору В. Лефевра [10], за допомогою *маніпулювання* здатністю до міжособистісного інформаційного обміну.

4. Рефлексивне управління *усвідомленням вибору* за допомогою *маніпулювання* здатністю до міжособистісного (невідомого спостерігачеві) інформаційного обміну за допомогою технологій психоінжинірингу [5].

Психоінжиніринг заснований на концепції багатошаровості свідомості людини і являється розвитком рефлексивних моделей. А. Денисов пояснює це наступним чином (подаємо із скороченнями): «Кожен шар свідомості знаходить своє вираження у зовсім специфічній системі інтерпретацій даних органами почуттів та образів реального світу. Кожен шар можна умовно представити як особливу квазіособистість або квазісвідомість, яка володіє специфічною картиною бачення світу. Людина може начебто переключатись з одного шару на другий, і ставати, тим самим, тимчасово то однією квазіособою, то другою, всякий раз змінюючи системи інтерпретації, які використовуються.

У свою чергу, кожна із систем інтерпретацій знаходить своє вираження у формуванні своєї особливої матриці цінностей. Рефлексивні моделі описують закономірності взаємодії свідомостей та вплив цих взаємодій на процеси прийняття рішень (морального вибору). Психоінжиніринг основну увагу приділяє вивченню закономірностей формування внутрішньої структури самої свідомості. Він дозволяє проводити пряме інженерне проектування колективної свідомості із новими, ще неіснуючими властивостями [5]».

Тепер, знаючи предмети і засоби управління, а значить і види інформації, необхідної для управління, ми можемо приступити до описування цілей і підходів до нової ієрархічної системи забезпечення кібербезпеки, адаптованої до ієрархічної системи управління. Приймемо припущення, що ієрархічна система забезпечення кібербезпеки має бути подібною до моделі ієрархічної системи засекречування, описаної в [5]. Це припущення витікає з того, що система засекречування визначає перелік інформації, яка підлягає захисту.

Системи захисту інформації, а далі системи інформаційної безпеки розвивались так, що базові принципи, методи і засоби, напрацьовані на попередніх етапах, не відкидаються, а залишаються, розширюються або удосконалюються, знаходячи собі свою нішу у нових комплексних системах інформаційної безпеки. При цьому, забезпечується принцип повноти і неперервності захисту. В ієрархічній системі кібербезпеки є чудова можливість – секрет верхнього рівня може на нижньому рівні розділятись. Тим самим можна понизити рівень захищеності кожного з розділених секретів. Це полегшує задачу оптимізації системи кібербезпеки.

Система забезпечення кібербезпеки має бути ієрархічною і мати чотири рівні. Підходи до ієрархічного забезпечення кібербезпеки пояснюються за допомогою рис. 1, де показані об'єкти забезпечення безпеки.

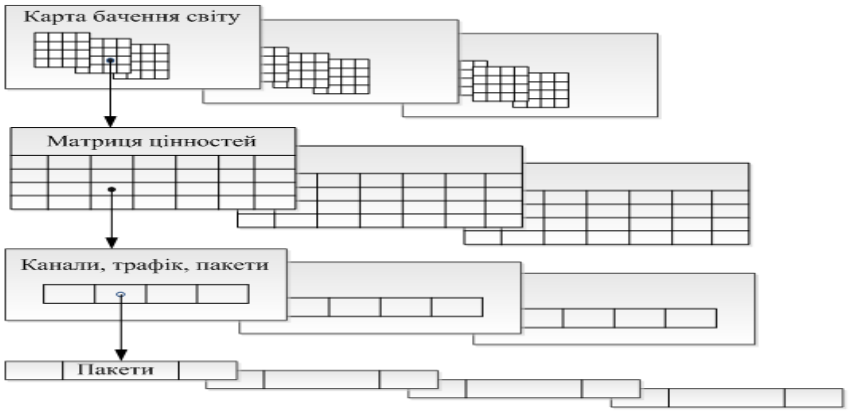

Рис. 1. Об'єкти ієрархічної чотири ступеневої системи забезпечення кібербезпеки

Цілі засекречування, по А. Денисову, (точніше об'єкти засекречування, а значить і об'єкти забезпечення кібербезпеки) розподілимо за рівнями системи засекречування наступним чином:

1. Засекречування інформаційних потоків.

2. Засекречування трафіку та каналів обміну інформаційними пакетами; засекречування моделей та технологій обміну інформаційними пакетами.

3. Засекречування матриць цінностей.

4. Засекречування картин бачення світу.

Що таке картина бачення світу інтуїтивно зрозуміло, але матриці цінностей вимагають свого пояснення.

Розглянемо концептуальні підходи до формування обрису перспективної інформаційно-управляючої системи цільового застосування та розвитку об'єднаних сил та засобів забезпечення національної безпеки (ИУС-НБ) [11, с. 497].

У основу розробки цієї системи буде покладено закон максимізації психологічного прибутку, який визначається перевищенням психічних доходів над психічними витратами. Останні залежать від сили і направленості індивідуальних та масових психічних переживань.

В ІУС-НБ покладається три базових принципи: рефлективності, екзістенційності та мережецентризму. Принцип рефлективності забезпечується використовуванням багатосторонніх багаторівневих стратегічних ділових ігор – моделей системи національної безпеки (МСНБ). Однією з основних частин стратегічних ділових ігор і є матриця цінностей.

«Принцип екзістенційності вимагає при розробці імітаційно-ігрової МСНБ поряд із матеріально-фізичними, психосоматичними та соціально-психічними факторами враховувати все розмаїття вищих смислових, месіанських, ментальних, архетипічних та духовно-моральних якостей усіх учасників системи внутрішньої та міжнародної безпеки. Іншими словами, кожен впливовий учасник системи національної безпеки має бути представленим в операційному просторі МСНБ (зокрема в матриці цінностей) [11, с. 497]».

Принцип мережецентризму, відносно до системи інформаційного управління національною кібербезпекою, полягає у доповненні вертикальних адміністративно-командних мережних структур управління горизонтальними неформальними, самоорганізованими мережними структурами громадського суспільства [13, с. 497].

Із принципу «мережецентризму» витікає застосування «організаційної зброї».

Застосування організаційної зброї може переслідувати конструктивні та деструктивні цілі. Конструктивні цілі полягають у створенні необхідних умов для створення у своєму середовищі стану «афективно-когнітивно-вольового консонансу – єдності розуміння, переживання та вольових відправлень у більшості його членів». Навпаки, деструктивні цілі – стану «афективно-когнітивно-вольового дисонансу», тобто напруженого конфлікту в сфері розуміння, переживання та волі у членів мережних структур, діяльність яких противна національним інтересам. Інструментом вибору стратегічних і оперативних рішень у сфері кібербезпеки являється використовування сукупності взаємодіючих між собою, розподілених, *багатосторонніх, багаторівневих стратегічних ділових комп'ютерних ігор*, які є *моделями системи національної безпеки* [11].

Повертаючись до рис. 1 приходимо до наступної системи чотириступеневої системи забезпечення кібербезпеки.

На першому рівні захищаються відомості, що закріплені в переліку інформації та інформаційних ресурсів, що захищаються. Цей рівень не зникає, а вдосконалюється, займаючи свої ніші в загальній системі кібербезпеки.

На другому рівні здійснюється сьогодні вже реалізований захист трафіку, моделей та технологій обміну інформаційним пакетами.

На третьому рівні забезпечується кібербезпека матриці цінності. Метод захисту – маніпулювання здатністю до міжособистісного інформаційного обміну. Прикладами є «Шоковий вплив на фінансові ринки. Управління (маніпулювання) противником. Методи внутрішньої валюти в рефлексивних іграх [1]».

На четвертому рівні можливо будуть застосовуватись методи забезпечення кібербезпеки картин бачення світу та відповідних, вироблених систем інтерпретації даних (зокрема, віртуальних), які сприймаються органами почуттів людини. Це ще потребує подальших глибоких досліджень.

Висновки

Запропоновано адаптивний підхід до побудови ієрархічної чотириступеневої системи кібербезпеки систем державного та суспільного управління, враховуючи можливі ознаки та властивості майбутнього суспільства високих технологій. Модель такої системи має чотири рівні: на першому рівні виконується забезпечення кібербезпеки інформаційних потоків; на другому – моделей та технологій обміну інформаційними пакетами; на третьому треба забезпечувати кібербезпеку матриці цінностей; на четвертому передбачається, що буде забезпечуватись кібербезпека картин бачення світу. Розроблений підхід дасть можливість проектувати більш гнучкі адаптивні системи забезпечення кібербезпеки ієрархічними систем.

Література

[1] Агеев А.И. Вектор перемен / А.И. Агеев, С.В. Авдеев, Рыжов В.Н. и др. // Экономические стратегии. – № 4, 2016. – С. 84-106.

[2] Путин использует бойню в Украине, чтобы репетировать войну с Западом / The Times, 10 августа 2016. [Электронный ресурс] – Режим доступа: http://glavnoe.ua/news/n279723.

[3] Стратегія кібербезпеки України / Указ Президента України від 15 березня 2016 р., №96/2016. – 11 с.

[4] Харченко В.П. Базова модель формування вимог до забезпечення кібербезпеки цивільної авіації / В.П. Харченко, О.Г. Корченко, С.О.Гнатюк // Ukrainian Scientificjournal of Information Security, 2016, Vol. 22, Issue 2, p. 150-155.

[5] Денисов А.А. Нетократия и рефлексия: Засекречивание в постиндустриальном обществе / А.А

Денисов // Рефлексивные процессы и управление. – Том 7, № 1, 2007. – С. 33 -50.

[6] Луцкий Г.М. Адаптивный подход к обеспечению безопасности распределенных компьютерных систем / Г.М. Луцкий, В.Е. Мухин // Вісник КДПУ імені Михайла Остроградського. Випуск 5/2007 (46). Частина 1. С. 30-34.

[7] Ализар А. Концепция адаптивной архитектуры безопасности от аналитика Garrtner / А. Ализар. 2014. [Электронный ресурс] – Режим доступа: https://xakep.ru/2014/07/09/adaptive-security-architecture.

[8] Корченко О.Г. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : Монографія / О.Г. Корченко, О.С. Архипов, Ю.О. Дрейс. – К.: наук.-вид. центр НА СБ України, 2014. – 332 с.

[9] Тарасюк М.В. Защита трафика инфокоммуникационных сетей и средств комп'ютерной разведки / М.В. Тарасюк // Защита информации. Инсайд. 2015, № 6. – С. 62-68.

[10] Лефевр В. Алгебра совести / В. Лефевр // Пер. с англ. – М.: «Когнито центр». 2003. – 55 с.

[11] Никитенко Е.Г. Облик перспективной информационно-управляющей системы обеспечения национальной безопасности России / Е.Г. Никитенко, Н.А. Сергеев // Оборонно-промышленный комплекс России. Т. 8. 2012. – С. 491-506. – Режим доступа: http://federalbook.ru/files/OPK/Soderjanie/OPK-8/V/Nikitienko.pdf.

УДК 003.26:004.056.55:621.39 (045)

Кононович В.Г., Стайкуца С.В., Кононович И.В., Копытин Ю.В., Романюков Н.Г. Адаптивные подходы к обеспечению кибербезопасности распределенных и иерархических систем управления

Аннотация. *Проблема кибербезопасности в условиях деструктивных информационных влияний является одной из острых проблем в современном и будущем обществах высоких технологий. Системы управления, как и информационные технологии, стали сверхсложными и интенсивно автоматизируются. В области государственного управления и управления информационным производством уровень критичности усиливается повышенным объемом обрабатываемой информации, распределенными интенсивными коммуникациями, иерархичностью систем и появлением новых потенциальных угроз. Существующие научные и практические работы не в полной мере учитывают современные требования нормативных документов по безопасности распределенных иерархических систем управления, не дают возможности учитывать для анализа и оценки безопасности управления поведением выбора и потребностей безопасности общества, порожденных новой материальной технологией в обществе высоких технологий. Исходя из этого, на базе исторического анализа трансформации основных подходов к защите информации, которая используется для управления, предложен адаптивный подход к построению иерархической четырех уровневой системы кибербезопасности: от обеспечения безопасности информационных пакетов и сведений, до обеспечения безопасности матриц ценностей и картин видения мира. В дальнейшей работе планируется разработка методов реализации подходов, сформированных в этой работе.*

Ключевые слова: *кибербезопасность, информационная безопасность, угрозы, общество высоких технологий, матрицы ценности, картины видения мира.*

Kononovich V., Staikutsa S., Kononovich I., Kopytin Yu., Romanyukov N. Adaptive approaches to cybersecurity of distributed and hierarchical management systems

Abstract. *The problem of cybersecurity in terms of destructive information impact is one of the acute problems in modern societies and the future of high technology. Management systems, as well as information technologies have become highly complex and intensely automated. In the field of public administration and management information critical production level is reinforced by the increased amount of information to be processed, distributed communications intensive, hierarchical systems and the emergence of new vulnerabilities and potential threats. Existing scientific and practical work does not fully take into account the current requirements of regulatory guidance documents on security of distributed and hierarchical control systems make it impossible to take into account the analysis and evaluation of safety management behavior of choice and security needs of society generated new material technology in a society of high technology. On this basis, on the base of historical analysis of transformation of the basic going near a privy, which is used managements, the adaptive going is offered near a construction hierarchical four levels of the system of cybersecurity: from providing of cybersecurity of informative packages and information to providing of safety of matrices of values and pictures of vision of the world. Futures papers will relate to methods of realization of approaches development for providing formed in this paper.*

Key words: *cybersecurity, information security, threats to society of high technology, information impact matrix values, world view pictures.*

Отримано *17 вересня 2016 року*, затверджено редколегією *8 жовтня 2016 року*