веден анализ угроз информационной безопасности и подробное описание источников преднамеренных угроз. Выполнен анализ уязвимостей информационной безопасности автоматизированных систем управления технологическим процессом, классификация и причины их возникновения. Даны рекомендации по устранению или нивелированию этих уязвимостей. Приведено выражение для определения вероятности реализации угроз информации. Исследованы взаимосвязи между угрозами, уязвимостями и риском для автоматизированных систем управления технологическим процессом. Приведен жизненный цикл вероятности реализации угроз информационной безопасности автоматизированных систем управления и сформулированы исходные данные, необходимые для данного анализа.
Ключевые слова: угроза, защита информации, автоматизированные системы управления технологическим процессом, уязвимости, риск, жизненный цикл.

ANALYSIS OF THE PROBABILITY IMPLEMENTATION OF THREATS PROTECTION OF INFORMATION IN INDUSTRIAL CONTROL SYSTEMS

For the purpose of the decision of the tasks connected to support of information security of industrial control systems the analysis of threats of information security and the detailed description of sources of deliberate threats is carried out. The analysis of vulnerabilities information security of the industrial control systems, classification and the reasons of their origin is made. Recommendations about elimination or leveling of these vulnerabilities are made. Expression for determination of probability of implementation of threats of the information is resulted. Correlations between threats, vulnerabilities and risk for the industrial control systems are researched. Lifecycle of probability of implementation of threats of information security of the industrial control systems is resulted and the initial data necessary for the given analysis is formulated.
Keywords: threat, information protection, industrial control systems, vulnerability, risk, lifecycle.

Гончар Сергій Феодосійович, кандидат технічних наук, заступник начальника державного науково-дослідного інституту спеціального зв'язку та захисту інформації.
E-mail: sfgonchar@yandex.ru
Гончар Сергей Феодосьевич, кандидат технических наук, заместитель начальника государственного научно-исследовательского института специальной связи и защиты информации.
Gonchar Sergii, PhD in Eng., Deputy Chief of State Research Institute for Special Telecommunication and Information Protection (Kyiv, Ukraine).

УДК 004.056.5: 004.738.5

ЗАХИЩЕНИЙ МЕРЕЖНИЙ ІНФОРМАЦІЙНИЙ РЕСУРС ЯК СИНЕРГЕТИЧНА СИСТЕМА

Володимир Блінцов, Денис Самойленко

Ускладнення сучасних мережних інформаційних ресурсів, впровадження у них інтелектуальних рішень з нелінійними зв'язками між елементами вимагає використання для їх опису адекватного математичного апарату. Наявні підходи, в основному, грунтуються на засобах системного аналізу, кібернетики, теорії ігор – детерміністичних математичних методах. Це обмежує можливості опису систем з великою кількістю елементів та принципово нелінійними зв'язками між ними, особливо у нерівноважних станах, які можуть виникати при спробі атак на інформаційні ресурси. Запропоновано структурну модель захищеного інформаційного ресурсу з архітектурою, що відповідає вимогам нормативної документації України та стандартів. У складеній моделі виявлено основні ознаки, типові для синергетичної системи. Використання математичного апарату синергетики дозволить більш якісно описати процеси, що супроводжуються виведенням системи з рівноваги, виділити ознаки наближення системи до точок біфуркації та розвинути засоби реалізації виведення системи з нерівноважних станів.
Ключові слова: *інформаційний ресурс, захист інформаційного ресурсу, захист сайту, модель інформаційного ресурсу, синергетика, синергетична модель.*

Постановка проблеми. Стрімка еволюція мережі Інтернет призводить до того, що ресурси цієї мережі, - сайти, - набувають усе більшої кількості функцій та обтяжуються усе більшою кількістю задач. Окрім функцій «візитної картки» чи довідника сучасні мережні інформаційні ресурси (МІР) виконують роль магазинів, банків та платіжних систем, відео- та телефонів, кінотеатрів, телебачення, радіостанцій, газет, журналів тощо. Додаткові завдання, пов'язані з управлінням іміджем власника МІР, маркетингом та соціальною спрямованістю, надають ресурсу «соціальних»

рис – МІР має «спілкуватись» з користувачем, причому це спілкування має бути приємним.

У той же час, економічна конкуренція надає перевагу тим, хто швидше розмістить власну інформацію у відкритій мережі. Досить часто поспіх у створенні МІР спряжений з недостатньою якістю впровадження захисних рішень, що, очевидно, може погіршити конкурентні переваги, здобуті за рахунок швидкого створення МІР. На перший план виходить задача розроблення рекомендацій та методик захисту МІР, доступних для швидкого використання. Також актуальною є задача постійного оновлення розробок, оскільки кожна з нових функцій МІР передбачає додаткову можливість негативного впливу на нього, а розширення функціональності являє собою визначальну тенденцію розвитку мережних ресурсів.

Через необхідність виконувати велику кількість різноманітних функцій МІР стає складним програмно-апаратним комплексом і, через цю складність, вимагає нових підходів до математичного опису та моделювання.

Аналіз останніх досліджень і публікацій. Основними підходами до моделювання процесів у інформаційних системах є методи системного аналізу, кібернетики і теорії ігор. У роботах [1-3] наведено огляд зазначених підходів та останні удосконалення у відповідних напрямах.

Зокрема, у роботі [1] розглянуто лише два стани інформаційної системи, при цьому математична модель з урахуванням нестаціонарних потоків була складена у вигляді системи диференціальних рівнянь. У роботі [2] у моделі запропоновано використання множин з розмірністю, відповідною розмірності множин вхідних дій та кількості власних параметрів. У роботі [3] встановлення значень параметрів моделі здійснюється граничним переходом до нескінченності.

З огляду на постійне збільшення функцій МІР, можна відзначити тенденцію зростання кількості складових елементів та розмірності множини вхідних параметрів, які відповідатимуть зверненням до функцій, що реалізують складові елементи. Так само збільшиться кількість станів системи, збільшуючи кількість диференціальних рівнянь у модельній системі. Можна стверджувати про досягнення певної логічної межі використання детерміністичних методів.

На підтвердження висловленого ствердження, у роботі [4] показана необхідність при моделюванні складних систем «звертатися до науково-методологічного інструментарію як кібернетики, так і синергетики». Відзначено, що «будь-який інший підхід є контрпродуктивним і неперспективним».

При розгляді питань захисту МІР слід відзначити про наявність нормативних документів з технічного захисту інформації України [5-7] та міжнародних стандартів, зокрема [8], положеннями яких регламентуються окремі рекомендації та вимоги, які прямо чи опосередковано стосуються самої структури МІР. При визначенні структурної моделі МІР та особливостей інформаційних потоків необхідно провести аналіз обмежень на архітектуру МІР.

Метою статті є аналіз вимог і обмежень на засоби захисту інформації у МІР, створення структурної моделі МІР з реалізованими засобами захисту інформації, виявлення у створеній моделі класичних синергетичних ознак.

Виклад основного матеріалу. Модель інформаційного ресурсу багато у чому залежить від кількості і характеру необхідних складових елементів чи функцій, наявність яких визначається технічним завданням чи бажанням власника ресурсу, однак, для ряду МІР регламентується діючими законами, стандартами та нормативними документами. Вимоги нормативів стосуються державних МІР, проте, є рекомендованими і для усіх інших.

Логічне та алгоритмічне наповнення ресурсу визначається, в основному, областю його використання та основним призначенням, вираженими у технічному завданні на його створення. Визначати спільні риси, характерні для МІР найрізноманітнішого призначення, з метою складання рекомендацій щодо алгоритмічної моделі МІР не вбачається за доцільне.

У той же час, до системи захисту інформаційних ресурсів, у т. ч. веб-сторінок, висувається ряд вимог, однаковий для ресурсів довільного алгоритмічного чи функціонального типу. Саме вимоги щодо побудови комплексної системи захисту інформації (КСЗІ) [5-7] визначатимуть спільні риси у моделях довільних МІР. Виділимо окремі норми, які впливатимуть на структурні особливості МІР. Оскільки КСЗІ передбачає ряд адміністративних та організаційних заходів, виділимо у предмет розгляду даної роботи лише заходи, пов'язані безпосередньо зі структурними та програмними заходами. Для уникнення невизначеності замість терміну КСЗІ будемо використовувати частинне означення – комплексну систему захисту інформаційного ресурсу (КСЗІР), як комплекс логічних, структурних, математичних, про-

грамних та інших засобів, реалізованих у програмному коді МІР.

Модульність [5: 8.2] вимагає створювати МІР у вигляді набору окремих модулів, які виконують власні функції і взаємодіють з іншими модулями через встановлені протоколи. Модульний принцип побудови програмного забезпечення, називаний також принципом приховування даних [9: 1.2.2], полягає у здійсненні такого розбиття програми на складові частини (модулі), за якого усі дані, з якими оперує модуль, були б визначені (приховані) у межах цього модуля. Гарним прикладом модульного принципу програмування виступає набір бібліотек функцій. Виділяється два принципи модульного програмування:

– принцип підвищення міцності модуля полягає у посиленні внутрішніх зв'язків у модулі. Розглядається 7 класів міцності: за збігами, за логікою, за класом, за процедурами, за комунікаціями, за функціями, за інформацією.

– принцип послаблення зчеплення модулів полягає у послаблені зв'язків між різними модулями. Аналіз проводиться за 5-ма класами зчеплення: за змістом, за областю, за керуванням, за форматом, за даними.

Ідеальною межею є модулі з абсолютною міцністю та нульовим зчепленням. Останнє призводить до необхідності виділення у окрему групу проблему взаємодії між модулями та головною програмою. Розв'язком проблеми виступають інтерфейси взаємодії – набір методів та властивостей, доступних для зовнішніх, по відношенню до модуля, програмних запитів.

Шаруватість [5: с.14, 8] рекомендує побудову МІР у вигляді шарів, кожен з яких взаємодіє лише зі своїми сусідами. КСЗІ має утворити зовнішній шар – оболонку, яка захищатиме внутрішні шари МІР. Міжнародним стандартом [8] виділено 7 рівнів (шарів) у найскладнішому випадку та надано рекомендації щодо поділу на меншу кількість шарів менш складних систем. У найпростішому випадку можна виділити лише два шари – оболонка КСЗІ та внутрішня частина МІР.

Диспетчер доступу [5: 8.3] рекомендується як невеликий модуль, який перевірятиме усі спроби доступу до системи. Диспетчер доступу можна уявити як певне вікно у захисній оболонці, крізь яке мають проходити усі запити користувачів до МІР.

З огляду на різновиди комунікаційної взаємодії сучасного МІР слід розширити концепцію диспетчера доступу. Перш за все, слід розділити взаємодію МІР з користувачами та іншими МІР, які по відношенню до даного називатимемо зовнішніми. Наприклад, такими МІР можуть бути засоби картографії, геопозиціювання, службами новин, реклами, точного часу, аудіо-, відеопрогравачі тощо. З метою уникнення перевантаження функціями диспетчера доступу, логічно виділити задачі взаємодії із зовнішніми МІР у окремий модуль комунікації, функціонально подібний до диспетчера доступу – модуль комунікації.

Комунікація з користувачами також може бути умовно поділена на статичну та динамічну. Статична взаємодія об'єднує стандартні методи запитів та передачі параметрів (GPC – Get, Post, Cookies). Статичною можна вважати взаємодію, ініційовану безпосередньо користувачем через введення адрес, відправлення форм чи переходу за посиланнями.

Динамічна взаємодія включає методи програмних (API) запитів, які генеруються програмним кодом клієнтської частини МІР і, як правило, приховані від користувача. Динамічні запити дозволяють оперативно оновлювати окремі частини веб-сторінки (синхронно чи асинхронно – AJAX) або перезавантажувати усю сторінку (reload). Логічним вважається розділення диспетчера доступу на два модулі, призначені для аналізу окремо статичних та динамічних запитів, оскільки ці запити мають принципові відмінності як за структурою, так і за видами атак, які через них реалізуються.

Самотестування [7: 7.2.14] вимагає наявності у системі функцій, метою яких є перевірка дієздатності системи. З урахуванням шаруватої структури МІР, модуль самотестування слід також розділити на два, які забезпечуватимуть функції внутрішнього та зовнішнього тестування.

Модуль внутрішнього тестування має функціонувати всередині захисної оболонки, перевіряючи дієздатність інформаційних модулів МІР. Тестування на стійкість до зовнішніх атак повинен забезпечити окремий модуль, завданням якого буде імітація дій нелегальних користувачів та зовнішніх МІР. З метою дотримання принципу заборони взаємодії через шар, модуль імітації зовнішніх дій має належати шару КСЗІ, у той час як модуль внутрішнього самотестування – до внутрішнього шару МІР.

Ідентифікація і автентифікація при обміні [7: 7.2.9-10] вимагає наявності у МІР засобів перевірки особи суб'єкта чи автоматизованої системи перед початком взаємодії. Засоби ідентифікації та автентифікації для статичної взаємодії логічно покладаються на диспетчер доступу та модуль комунікації.

Динамічна взаємодія з користувачами та зовнішніми МІР передбачає періодичне повторення запитів та оброблення відповідей. Оскільки авторизація користувача чи ідентифікація ресурсу не повинні повторюватись при кожному запиті, логічно виділити окремі процедури автентифікації користувачів та ресурсів, задачею яких буде унеможливлення підміни запитів іншими (нелегальними) користувачами чи ресурсами. З метою логічного поділу запитів прихованої автентифікації та динамічного обміну за задачами та методами, зазначені процедури та дані, з якими вони оперують, слід відокремити у самостійні модулі – фонової чи прихованої автентифікації користувачів/МІР.

Конфіденційність при обміні [7: 7.2.2] вимагає, зокрема, забезпечення захисту об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Безпосереднє виконання цієї вимоги має супроводжуватись введенням модуля криптографічних перетворень для даних з обмеженим доступом. З метою покращення інформаційної безпеки МІР цей модуль має бути розміщений у комунікаційній ланці найглибшого інформаційного обміну – у складі модуля взаємодії з базою даних МІР.

З урахуванням наведених вимог до захисних функцій МІР можна запропонувати структурну схему, наведену на рис. 1. Пунктирною лінією зазначено «захисну оболонку» МІР – логічну межу зовнішнього архітектурного шару. Модулі, які реалізують «вікна» у оболонці зображені поряд з оболонкою і належать зовнішньому шару. Функціональним призначенням зовнішнього шару є оброблення (аналіз) запитів від зовнішнього середовища.

Модулі внутрішнього шару забезпечують реалізацію запитів після аналізу у зовнішньому шарі, а також функції самотестування. Задля спрощення рисунка не зазначено усі зв'язки між модулями, проте вважається, що усі модулі МІР мають зв'язок з базою даних (чи базою знань) та модулем самотестування. У окрему під-оболонку виділено засоби доступу до даних – базу даних та модуль криптоперетворень для інформації з обмеженим доступом.

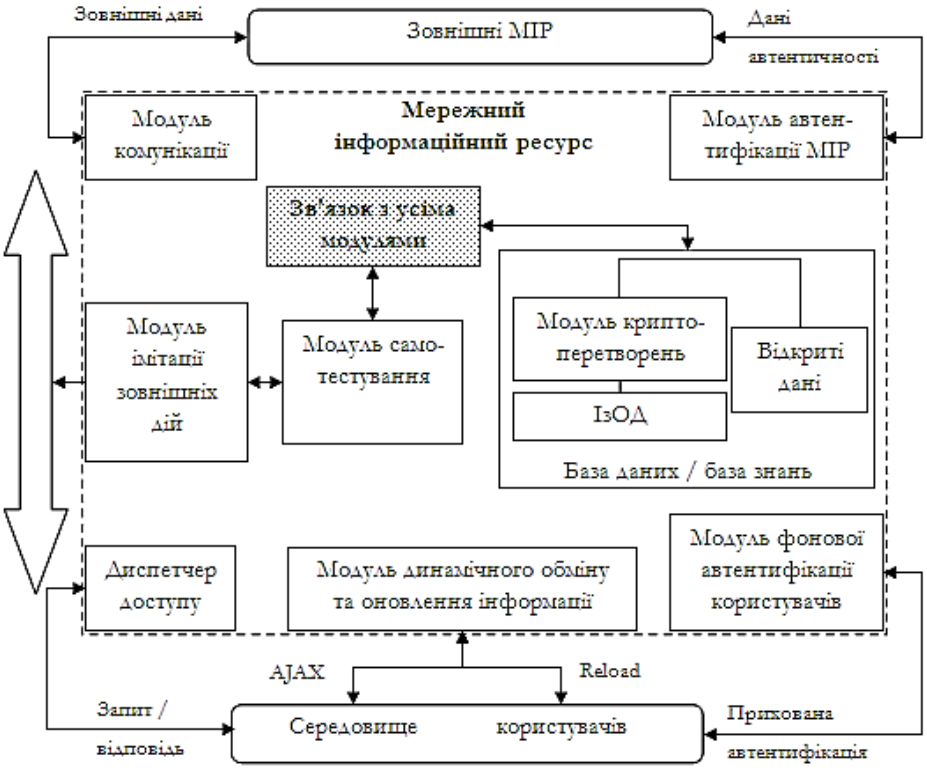

Рис. 1. Модульна структура МІР з КСЗІР

Для виділення у МІР синергетичних рис слід розглянути основні особливості об'єктів вивчення синергетики [10-11] та стохастичного управління [12]. Серед властивостей синергетичних систем (СС) основними є відкритість, складність, нелінійність, наявність нерівноважностей та біфуркаційного механізму.

Відкритість системи передбачає її тісну взаємодію з оточенням. СС виникають лише у потоці і зникають при його припиненні. Так у енергетичному потоці тепла з'являються комірки Бе-

нара, у потоці речовини (концентрації) виникає реакція Бєлоусова-Жаботинського. Людину теж можна вважати структурою, що існує у потоці речовин і без нього існувати не може [10-11].

Принцип функціонування МІР повністю відповідає описаній вимозі. МІР активізується лише при надходженні запитів і припиняє активність при їх відсутності – МІР функціонує у інформаційному потоці. Вимога відкритості принципово властива довільному мережному ресурсу. Без запитів користувачів (без інформаційного потоку) МІР – це лише набір файлів на якомусь сервері. Більшу деталізацію потоків можна побачити на рис. 1.

Складність системи вимагає наявності у системі великої кількості елементів, що взаємодіють між собою.

Складність МІР, як вже зазначалось, зростає з еволюцією інформаційних технологій і на теперішній час може вважатись достатньою для синергетичного опису. Кількість динамічних об'єктів у звичайному сучасному, відносно популярному МІР може сягати мільйонів. Сервери пошукових сервісів можуть витримувати інформаційні потоки у сотні Гб/с, опрацьовуючи мільярди запитів і створюючи десятки мільярдів динамічних об'єктів щосекунди. Наявність КСЗІР з модульно-шаровою архітектурою забезпечує необхідність взаємодії цих об'єктів на всіх етапах життєвого циклу.

Нелінійність передбачає наявність нелінійних зв'язків між елементами системи.

Достатньо очевидно, що складові елементи МІР, – як статичні, так і динамічні, – пов'язані між собою нелінійним чином. У ряді випадків зв'язок має порогову нелінійність – при одному сигналі з модуля автентифікації комунікація підтримується, при іншому припиняється. Якщо МІР має більш складну шарувату архітектуру і процес автентифікації розподілений за кількома шарами, то нелінійність зв'язків тільки посилюється. Практично для кожного модуля МІР з наведених на рис. 1, зв'язок входу і виходу не можна описати лінійною функцією.

Нерівноважність полягає у наявності кількох стійких станів (атракторів) СС, перехід між якими відбувається при флуктуаціях потоку (зовнішньої дії). Додатково передбачається дія біфуркаційного механізму, тобто наявності таких станів системи, вихід з яких повністю непередбачуваний і украй чутливий до незначних зовнішніх змін. У нестійких станах проявляється взаємодія віддалених елементів, а не лише сусідніх [10-11].

Властивість нерівноважності властива усім МІР із функціями захисту. Стійкі стани відповідають стаціонарним легальним потокам з підтвердженими параметрами захисту. При незначних відхиленнях (флуктуаціях, шумах) у інформаційних потоках можливі порушення у процесі оброблення запитів. Наприклад, перевірка на чутливість МІР до SQL-ін'єкцій здійснюється додаванням до запиту одного зайвого символу чи підміною одного символу з легального запиту, тобто мінімально можливими змінами у запиті, які цілком справедливо можна вважати флуктуаціями. До того ж подібні флуктуації можуть походити від перешкод при передачі сигналів.

Якщо засоби захисту пропустять флуктуацію до внутрішніх шарів, то спроба оброблення невірного запиту ініціює помилки у цих шарах, а відтак спровокує взаємодію через шари. У прикладі з SQL-ін'єкцією помилка виникне у найнижчому шарі, у якому зберігаються основні дані МІР – база даних. Відповідно, міжшаровий ефект досягне максимального значення.

У разі успішної атаки, МІР перейде у інший стаціонарний стан, бажаний для зловмисника. Несанкціонований доступ (НСД) можна вважати найбільш типовим прикладом переходу МІР у такий стан. З одного боку, МІР функціонує, оскільки НСД до непрацюючого МІР неможливий принципово. З іншого боку, функціонує у невірний спосіб. Описана ситуація повністю подібна до біфуркаційної поведінки, за якої незначні зміни у потоці можуть спровокувати перехід системи у інший стан чи взагалі припинити її функціонування.

Відтак наявність точок біфуркації може свідчити про недоліки у будові КСЗІР, а пошук таких точок стає неодмінною задачею випробувачів захищеності МІР.

Описані властивості МІР засвідчують повну відповідність особливостям синергетичних систем. Це обумовлює можливість опису МІР як СС із застосуванням до його моделі засобів стохастичного (не детермінованого) керування.

Одним з принципів стохастичного керування є твердження про те, що ступінь невизначеності процесу не може бути зменшена у процесі його оброблення [12]. Цей принцип накладає певні принципові обмеження на функціонування КСЗІР, зокрема, унеможливлює гарантовано вірне оброблення запиту, підверненого дії шумів чи спотворень. Це може виступати обґрунтуванням впровадження засобів перешкодостійкого коду-

вання або перегляду політики безпеки щодо гарантування доступності МІР.

Оскільки математичний апарат синергетики є універсальним для систем довільної природи, цей апарат може бути застосований для моделювання захищеного МІР довільного функціонального призначення, з довільною програмною парадигмою та логікою оброблення даних. Перспективним вбачається встановлення інформаційного сенсу параметрів рівнянь типових синергетичних моделей у випадку використання їх для опису поведінки МІР.

Висновки. Запропонована структурна модель типового мережного інформаційного ресурсу із комплексною системою захисту інформації за модульним принципом та шаруватою архітектурою. Виділено ряд програмних модулів МІР, розподілених за двома архітектурними шарами.

Показана відповідність МІР, як складної цілісної системи, до об'єктів синергетики за основними ознаками: відкритістю, складністю, нелінійністю та нерівноважністю. Обґрунтовано застосування для опису та аналізу моделей МІР засобів синергетики та стохастичного керування.

Перспективи подальших розвідок вбачаються у адаптації синергетичних моделей до опису МІР з функціями захисту, виявленню їх принципових обмежень та змісту у інформаційному просторі.

ЛІТЕРАТУРА

[1]. Грищук Р. В. Р-моделювання процесів нападу на інформацію при нестаціонарній природі потоків захисних дій та інформаційних атак. [Текст] / Р. В. Грищук // Системи обробки інформації, 2009. – випуск 7 (81). – с. 98-101

[2]. Висоцька В. Математичні моделі інформаційних потоків у системах електронної контент-комерції [Електронний ресурс] / В. Висоцька // Електронний науковий архів Науково-технічної бібліотеки Національного університету "Львівська політехніка"": – Режим доступу http://ena.lp.edu.ua:8080/bitstream/ntb/8055/1/28.pdf (дата звернення: 01.12.13)

[3]. Бойко Н. Моделювання web-орієнтованих систем та напрямки розвитку web-ресурсів [Електронний ресурс] / Н.І. Бойко // Електронний архів Національної бібліотеки України імені В. І. Вернадського. – Режим доступу http://archive.nbuv.gov.ua/portal/natural/vnulp/ISM/2012_743/02.pdf (дата звернення: 01.12.13)

[4]. Ожеван М. А. Синергетика проти кібернетики: конкурентні методологічні підходи до моделювання складних соціальних систем [Текст] / Ожеван М. А. // Стратегічні пріоритети. – 2012. - № 3 (24). – с. 126-133.

[5]. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Text] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

[6]. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Text] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

[7]. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. [Text] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

[8]. ISO/IEC 7498-1:1994(E) Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. [Text] / ISO/IEC 7498-1:1994(E). Second edition. Corrected and reprinted 1996. Switzerland: ISO/IEC Copyright Office. – 68 p.

[9]. Страуструп Б. Язык программирования С++. [Текст] / Бьерн Страуструп. – М.: Бином, Невский Диалект. – 2008. – 1104 с.

[10]. Хакен Г. Синергетика. [Текст] / Хакен Г. – М.: Мир. – 1980. – 405 с.

[11]. Степин В. С. Синергетика и системный анализ. [Текст] / Степин В. С. // Синергетическая парадигма. Когнитивно-коммуникативные стратегии современного научного познания. М.: Прогресс-Традиция. – 2004. – 560 с.

[12]. Саридис Д. Н. Самоорганизующиеся стохастические системы управления. [Текст] / Саридис Д. Н. – М.: Наука. – 1980. – 400 с.

REFERENCES

[1]. R.V. Gryschuk (2009) P-simulation of the attack process on the information with the non-stationary kind of the protective and information attack. *Information processing systems* 7 (81), p. 98-101.

[2]. Vysotska V. (2010) Mathematical models of information streams in e-commerce systems [Online] Scientific library of Lviv Polytechnic. Available from http://ena.lp.edu.ua:8080/bitstream/ntb/8055/1/28.pdf [Accessed: 1st December 2013].

[3]. Boyko N. (2012) Web-oriented systems modeling and web-resources development direction. [Online] E-archive of National Library of Ukraine. Available from http://archive.nbuv.gov.ua/portal/natural/vnulp/ISM/ 2012_743/02.pdf [Accessed: 1st December 2013].

[4]. Ozhevan M. A. (2012) Synergetic versus cybernetics: concurrent methodological approach to complex social system modeling. *Strategic Priority*. 3 (24), p. 126-133.

[5]. UKRAINE Security Service of Ukraine (1999) General statements on information security in computer systems from unauthorized access (1.1-002-99). Kyiv: SSU.

[6]. UKRAINE Security Service of Ukraine (1999) Estimation criteria of information security in computer

systems from unauthorized access (2.5-004-99). Kyiv: SSU.
[7]. UKRAINE Security Service of Ukraine (2004) Requirements for information security of WEB-page from unauthorized access (2.5-010-2003). Kyiv: SSU.
[8]. ISO/IEC 7498-1:1994(E) Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. Second edition. Corrected and reprinted 1996. Switzerland: ISO/IEC Copyright Office, 68 p.
[9]. BJARNE STROUSTRUP (2008) *The C++ Programming Language*. Moscow: Binom.
[10]. HERMANN HAKEN (1980) *Synergetic* Moscow: Mir
[11]. Stepin V. S. The synergetic and the system analysis. In ARSHINOV et al. (ed.) (2004) *Synergetic paradigm*. Moscow: Progress-Tradition.
[12]. SARIDIS D. N. (1980) *Self-organizing stochastic control systems*. Moscow: Science.

ЗАЩИЩЕННЫЙ СЕТЕВОЙ ИНФОРМАЦИОННЫЙ РЕСУРС КАК СИНЕРГЕТИЧЕСКАЯ СИСТЕМА

Возрастающая сложность современных сетевых информационных ресурсов, внедрение в них интеллектуальных решений с нелинейными связями между элементами требует применения для их описания адекватного математического аппарата. Существующие подходы, в основном, базируются на средствах системного анализа, кибернетики, теории игр – детерминистических математических методах. Это ограничивает возможности описания систем с большим количеством элементов и принципиально нелинейными связями между ними, особенно в неравновесных состояниях, возникающих при попытках атак на информационные ресурсы. Предложена структурная модель защищенного информационного ресурса с архитектурой, соответствующей требованиям нормативной документации Украины и стандартов. В модели обнаружены основные признаки, типичные для синергетической системы. Применение математического аппарата синергетики позволит более качественно описать процессы, сопровождающиеся выходом системы из равновесного состояния, выделить признаки приближения системы к точкам бифуркации и разработать средства, реализующие выведение системы из неравновесных состояний.

Ключевые слова: информационный ресурс, защита информационного ресурса, защита сайта, модель информационного ресурса, синергетика, синергетическая модель.

SECURED NETWORK INFORMATION RESOURCE AS SYNERGETIC SYSTEM

The increasing complexity of modern network infomation resources, the introduction of intelligent program solutions with non-linear relationships between elements requires the use adequate mathematical tools to describe them. Existing approaches are mainly based on the means of systems analysis, cybernetics, game theory - deteminitic mathematical methods. This limits the ability to describe systems with a large number of elements and essentially with non-linear relationships between them, especially in non-equilibrium states, caused by attacks attempting on information resources. A structural model of protected information resources with the architecture conforming to the requirements of normative documentation of Ukraine and standards were proposed. The model shows the main features that are typical for a synergetic system. Application of synergetic mathematical methods will allow describing more qualitatively the processes of system deviation from equilibrium state, detecting features of the system approaches the bifurcation point, and developing tools for system diversion from non-equilibrium states.

Keywords: information resource, secured information resource, website security, information resource model, synergetic, synergetic modeling.

Блінцов Володимир Степанович, доктор технічних наук, професор, проректор з наукової роботи, завідувач кафедри електрообладнання суден та інформаційної безпеки. Національний університет кораблебудування імені адмірала Макарова.
E-mail: volodymyr.blintsov@nuos.edu.ua
Блинцов Владимир Степанович, доктор технических наук, профессор, проректор по научной работе, заведующий кафедрою электрооборудования суден и информационной безопасности. Национальный университет кораблестроения имени адмирала Макарова.
Blintsov Volodymyr, doctor of technical sciences, professor, vice-rector for scientific work, head of Ship Electrical Equipment and Information Security Department, National University of Shipbuilding after Admiral Makarov.

Самойленко Денис Миколайович, кандидат фізико-математичних наук, доцент, доцент кафедри електрообладнання суден та інформаційної безпеки. Національний університет кораблебудування імені адмірала Макарова.
E-mail: DenNikSam@gmail.com
Самойленко Денис Николаевич, кандидат физико-математических наук, доцент, доцент кафедры электрооборудования суден и информационной безопасности. Национальный университет кораблестроения имени адмирала Макарова.
Samoilenko Denis, PhD, docent of Ship Electrical Equipment and Information Security Department, National University of Shipbuilding after Admiral Makarov.