УДК 003.26:004.056.55:621.39(045)

ИНТЕГРАЦИЯ СИСТЕМ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ

Стайкуца С.В.
Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная,1.
s.staikuca@gmail.com

ІНТЕГРАЦІЯ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЙНИХ І МАТЕРІАЛЬНИХ ЦІННОСТЕЙ

Стайкуца С.В.
Одеська національна академія зв'язку ім.О.С.Попова,
65029, Україна, м. Одеса, вул. Ковальська,1.
s.staikuca@gmail.com

INTEGRATION OF THE SYSTEMS SAFETY INFORMATIVE AND MATERIAL VALUES

Staikuca S.V.
O.S. Popov Odessa national academy of telecommunications
1 Kovalska St., Odessa, 65029, Ukraine
s.staikuca@gmail.com

Аннотация. В статье предложено интегрировать систему охраны и защиты информационных и материальных ценностей (ресурсов) в организациях, учреждениях и предприятиях. Разработана модель динамики процессов в системе защиты ценностей с запаздыванием принятия управленческих решений. Полученные результаты позволяют повысить эффективность работы интегрированных систем охраны и защиты информационных и материальных ценностей и формализовать направления дальнейших исследований по разработке новых эффективных систем охраны и защиты ресурсов с использованием интегральных технологий.

Ключевые слова: защита информации, нелинейная динамика, модель систем с задержкой, антивирусная защита, интеграция, система охраны.

Анотація. У статті запропоновано інтегрувати систему охорони та захисту інформаційних і матеріальних цінностей (ресурсів) в організаціях, установах і підприємствах. Розроблено модель динаміки процесів у системі захисту цінностей із запізнюванням прийняття управлінських рішень. Отримані результати дозволяють підвищити ефективність роботи інтегрованих систем охорони та захисту інформаційних і матеріальних цінностей та формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем охорони та захисту ресурсів з використанням інтегральних технологій.

Ключові слова: захист інформації, нелінійна динаміка, модель систем із затримкою, антивірусний захист, інтеграція, система охорони.

Abstract. In paper proposed to integrate the system of guard and security of information and material values (resources) in organizations, establishments and enterprises was proposed. A model of the dynamics of processes in the system of security of values with the delays of acceptance of administrative decisions is developed. The obtained results allow to improve the efficiency of work of the integrated systems of guard and security of information and material values. It also allows formalize directions for further research on the development of new effective systems of protection and security of resources using integral technologies.

Key words: information security, criminality, nonlinear dynamics, model of the systems time-lagged, anti-virus defence, integration, protect system.

За даними Міжнародного Союзу Електрозв'язку спостерігається експоненційний характер зростання кіберзлочинності [1]. Кількість інцидентів з інформаційною безпекою зростає в геометричній прогресії [2]. Атаки стають складними та витонченими. Кількість нових шкідливих програм у мережах налічуються мільйони. А згідно із законом У. Росс Ешбі щодо необхідного різноманіття: "Кількість регулювання має бути не меншою

різноманітності збурень, проти якого направлене регулювання" [3, с. 293...296, 346; 4, с. 63...64]. Складність поведінки системи протидії повинна перевищувати складність поведінки атакуючої системи. Звідси випливає й висловлювання Є.А. Касперського щодо «важливості складних технологій (безпеки) в епоху складних атак» [5].

Загальною проблемою є удосконалення та підвищення ефективності систем захисту інформації і систем охорони інформаційних цінностей в організаціях, установах і підприємствах.

Для багатьох організацій захищеність мережі стає одним із найважливіших пріоритетів. Системи безпеки стають складними, про що свідчать численні публікації, наприклад [6…9]. З іншого боку, у багатьох сферах, які характеризуються підвищеною складністю, спостерігаються процеси інтеграції, конвергенції й уніфікації, які спонукаються застосуванням і розповсюдженням інформаційних технологій. Наприклад, телекомунікації у своєму розвитку пройшли шлях від індивідуальних мереж для кожного виду зв'язку – телефонних, телеграфних, передачі даних, фототелеграфних, радіомовлення тощо, до цифрової конвергованої телекомунікаційної мережі, в якій передаються аудіо, відео, дані, телефонні розмови. На черзі – передача цифрового телебачення уніфікованою мережею загального користування [10, с. 36; 11]. Інтегральний підхід «до множини різних ризиків» безпеки декларується в [4, с. 36]. Інтеграція систем безпеки може дати відчутний економічний виграш.

Назріла необхідність прояснити її можливості, задачі та необхідності. Незважаючи на розвиненість теорії, методик і техніки безпеки стан інформаційної безпеки, не можна вважати задовільним. Не останньою причиною цього є «людський фактор» і, зокрема, запізнювання в прийнятті нагальних рішень. Запізнювання виникає і як технологічне явище (за час одного покоління змінюють одна одну декілька технологій, що непередбачено виявилися вразливими. Потрібен час для вироблення протидії), і як соціальне явище (наприклад, за необхідності навчання користувачів, фахівців та осіб, що приймають рішення. Люди, особливо старшого віку, можуть мати труднощі з перенавчанням і сприйманням нових загроз), і як психологічне явище (має місце звикання до технологій і недооцінка ризиків. Людський фактор став однією із важливих проблем безпеки і досліджений поки що недостатньо глибоко).

Метою даної статті є підвищення ефективності роботи систем охорони матеріальних цінностей і систем захисту інформації за рахунок їх інтеграції та побудови динамічної моделі процесів у системі захисту цінностей із запізнюванням прийняття управлінських рішень.

Кожне підприємство, організація, установа має певну систему обліку, експлуатації, охорони матеріальних і виробничо-технічних цінностей. Існують певні правила та інструкції щодо охорони, експлуатації, зберігання та переміщення цінностей. Призначаються матеріально відповідальні особи, періодично за регламентом проводяться інвентаризації, ревізії тощо. Елементами цієї системи є вахтери, коменданти, замки, сейфи та ін. Із захистом інформації у цій системі не виникало проблем. Інформація зберігалась і оберталась на твердих фізично чутливих носіях: книги зберігались у бібліотеках, інструкції, накази – в папках у шафах на полицях, відомості щодо кадрів – у картотеках і т.п. Передати інформацію означало передати документ, ознайомитись з інформацією означало прочитати документ і повернути його на місце. Контроль збереженості документа зводився до перевірки наявності документа: у загальному випадку – до перевірки збереженості його носія. Інформацію носія можна було побачити, поторкати, перевірити чи не зіпсувався носій. Інформацію можна було спалити, порвати або порізати на шматки. Існуючі закони, правила охорони, використання, зберігання, контролю тощо матеріальних цінностей були автоматично перенесені на інформаційні носії. «Інформація – особливий ресурс, що відрізняється від матеріальних ресурсів. Існуючі концепції оцінки інформації, інтелектуальної власності, за суттю, є застосуванням принципів, які розроблені стосовно матеріальних ресурсів [12]». Інформація, як окрема цінність, охоронялась як документи.

З появою та розповсюдженням інформаційних технологій (ІТ) інформація, крім свого фізичного матеріального аспекту у вигляді запису на твердому носії, отримала новий аспект – віртуальність у вигляді послідовності цифр, що знаходяться десь в пам'яті у середині машини і які не можна побачити, прочитати, послухати без спеціальних засобів комп'ютерної техніки. У зв'язку з цим звернемо увагу на проблему охорони та захисту інформації із виробничого, термінологічного та правового аспектів.

Виробнича сторона захисту інформації. Раніше інформація, документи та дані відігравали, в основному, допоміжну обслуговуючу функцію в матеріальному виробництві, управлінській та культурній діяльності, торгівлі тощо. Інформація (документи) відображала матеріальні об'єкти. За кожним документом стояв певний предмет, процес або діяльність. Без документів будь-яка виробнича або інша діяльність неможлива. «Розробка, планування й організація виробництва та саме виробництво будь-якого товару та послуги використовує, крім матеріальних ресурсів, ще й інформаційні ресурси, принципи економічної оцінки яких знаходяться тільки у початковій стадії розробки [12]».

Цінність інформації визначалась і була складовою цінності тих засобів і продуктів діяльності, які ця інформація обслуговувала. На відміну від цього, тепер, крім зазначеної обслуговуючої ролі, що залишається повною мірою, віртуальна інформація набула і самостійної ролі. Вона сама тепер стала продуктом, товаром, засобом виробництва, і, природно, сировиною інформаційного виробництва. Це означає, що інформація стала мати ще й свою власну цінність поза зв'язком із матеріальним виробництвом або іншою традиційною діяльністю. Крім матеріально-технічних цінностей з'явились інформаційні цінності. Захист інформації стали виділяти як окрему функцію забезпечення безпеки (охорони). Характерним прикладом цього є прийняття Закону України «Про захист персональної інформації» та низка законодавчих актів про комерційну таємницю.

Термінологічна сторона захисту інформації. Прийнята термінологія в напрямі інформаційної безпеки дещо заплутує ситуацію із поняттям захисту інформації. Термін «Захист інформації» виник у рамках охорони державної таємниці. У системі охорони державної таємниці, її невід'ємною частиною, є охорона документів, що містять інформацію з обмеженим доступом. У цілому, захист інформації з обмеженим доступом здійснюється системами криптографічного захисту інформації, технічного захисту інформації та системою організаційно-технічних заходів, яка нині з розвитком ІТ вийшла на рівень управління інформаційною безпекою. У рамках технічного захисту інформації також виділилась система інформаційної безпеки інформаційно-комунікаційних систем. За такою класифікацією поза увагою може опинитись захист тих інформаційних цінностей, що не відносяться до інформації з обмеженим доступом – так званої «відкритої інформації».

Із поняттям «Захист інформації» звикли пов'язувати контекст секретності. Захист інформацій асоціюється в багатьох випадках як захист інформації з обмеженим доступом. Тому в термін «Захист інформації» важко тепер внести розуміння його як охорону, наприклад, ще й відкритої інформації, яка теж має свою цінність. Не даремно виник новий термін «Інформаційна безпека», який краще асоціюється із задачами охорони електронної інформації. Доцільно вважати синонімами терміни «Захист інформації» і «Охорона інформації» безвідносно до її поділу на відкриту інформацію та інформацію з обмеженим доступом.

Віртуальна сторона захисту інформації. Інформаційні технології змінили природу документа. Документ, який охоронявся, який був, фактично, матеріальною цінністю, перетворився в потік електронів – документ став віртуальним. Його не можна поторкати, відчути і побачити його можна тільки за допомогою технічних засобів. Документообіг стає безпаперовим і нематеріальним. Бухгалтерія функціонує за допомогою комп'ютерної мережі. У деяких країнах – Канаді, Республіка Корея, Естонія, функціонують Електронні уряди.

Електронний документ стало легко створювати, необмежено копіювати, змінювати, доповнювати, знищувати. Інформація, на відміну від матеріального ресурсу, з мінімальними витратами зберігається, транспортується, необмежено копіюється та необмежено використовується. Але за електронним документом, як і раніше, у матеріальному світі стоїть певний об'єкт, процес і навіть суб'єкт. Вони (віртуальний документ і матеріальний об'єкт, який він відображає), як і раніше, тісно пов'язані між собою. Зміни в документі неодмінно тягнуть за собою зміни в матеріальному світі і навпаки. Тому захист віртуальної інформації, її охорона, стали важливою частиною діяльності людини. Розуміння цієї необхідності ще не стало повним як у технічних фахівців, так і в управлінців, так і в осіб, що приймають рішення.

Передумови та необхідність інтеграції системи охорони матеріально-технічних цінностей та системи захисту інформаційних цінностей. Документ, який існує як дещо, що знаходиться в пам'яті комп'ютера, можна роздрукувати. Тоді він попадає у систему охорони матеріальних цінностей. При цьому, ми не можемо не приділити увагу питанню охорони електронних документів і, взагалі, електронної інформації. Потрібно охороняти (захищати) документи (інформацію як цінність) на всіх етапах життєвого циклу документів, зокрема на етапах їх існування як у паперовому, так і в електронному вигляді. Можна і потрібно охороняти комп'ютери як інвентарні матеріальні цінності. Але комп'ютер – це просто «електронна шафа» із засобами автоматизації роботи з інформацією (документами).

У комп'ютері зберігаються і обробляються тисячі й мільйони документів. Електронний документ повинен мати свій «інвентарний номер» як інформаційна цінність. Потрібна система охорони електронних документів, правила доступу та обробки документів, аналогічні системам, правилам і законам роботи з паперовими документами. Прикладом такої системи є система обробки бухгалтерської інформації 1С.

Інформаційні цінності проявляються двояко – як матеріальний об'єкт, коли інформація записана на твердому носії, і як віртуальний об'єкт, коли вони зберігаються і обробляються в електронному вигляді. Отже, є вагомі об'єктивно природні причини створення єдиної інтегрованої системи охорони (захисту) інформаційних і матеріальних цінностей. Запорукою такого рішення є те, що ІТ вторгаються в усі сфери діяльності, зокрема, у сферу охорони матеріальних цінностей, де запроваджуються автоматизовані системи сигналізації, відеоспостереження, контролю доступу тощо.

Система, правила, процедури роботи з електронними документами дещо інші, ніж відповідні процедури роботи з матеріальними цінностями. Можна запропонувати два варіанти вирішення цієї проблеми:

1. Створити окрему службу та систему захисту електронних документів (інформації) та розробити для них нормативно-правові документи: політику захисту, правила розмежування доступу, зберігання й оброблення інформації. Для цього створюється й удосконалюється законодавчо-нормативна та нормативно-правова база, а також програмно-технічна база, проводиться підготовка спеціалістів. Недолік цього варіанта полягає в порівняно великих витратах, що можуть для системи інформаційної безпеки досягати 15...20 % від витрат на ІТ залежно від цінності інформації, що захищається.

2. Реорганізувати існуючу службу і систему охорони, експлуатації, зберігання, обліку, контролю матеріальних цінностей, залучивши до неї фахівців ІТ та інформаційної безпеки, або провівши навчання старих фахівців у системі курсів підвищення кваліфікації. Тим самим вона перетвориться у службу охорони (захисту) інформаційних та матеріальних цінностей. Передумовою такої інтеграції є все більше проникнення ІТ у службу охорони. У табл. 1 показані порівняльні переліки деяких функцій фахівців, які повинні набути «подвійної» спеціалізації.

Таблиця 1 – Подвійна спеціалізація служби інформаційної безпеки та служби захисту й охорони

Функції охорони матеріальних цінностей	Функції охорони інформаційних цінностей
Керівництво	Керівництво
Робота з персоналом	Робота з персоналом
Адміністрування, розпорядництво	Системне адміністрування
Матеріальна відповідальність	Адміністрування безпеки
Правила роботи, охорони та службові обов'язки	Правила доступу та ролі, захист цілісності та доступності
Правила зберігання та обліку матеріальних цінностей	Правила зберігання архівних, резервних та робочих копій
Технічні засоби охорони	Система захисту інформації
Облік роботи	Журнал дій (лог-файли)
Контроль засобів охорони	Аудит безпеки
Техніка безпеки та санітарні норми	Антивірусний захист і захист від опромінювання

Перелік функцій не є повним і наводиться як приклад. Недоліком другого варіанта є необхідність перенавчання фахівців і освоєння ними нових функцій, знань та умінь. Але це стає нормою практично в усіх сферах діяльності людини внаслідок швидкої зміни нових технологій.

При цьому зволікання з прийняттям рішень щодо захисту інформації може призвести до неочікуваних втрат або збитків. Це можна довести з математичною точністю за допомогою моделей, які досліджуються методами нелінійної динаміки та комп'ютерного моделювання. Розглянемо вплив запізнювання з прийняттям рішень на роботу систем забезпечення інформаційної безпеки.

Прийняття рішень в управлінні, як і функціонування багатьох природних і технічних систем проводиться із запізнюванням. Такі системи називають системами із запізнюванням. У них результат впливу виявляється не відразу, а через певний час τ – час запізнювання. Доведено, що для таких систем характерні циклічні процеси – автоколивання. Розглянемо за допомогою методів синергетики наслідки цього явища на прикладі захисту від вірусних атак та інших інцидентів з інформаційною безпекою.

В економічних, біологічних, технічних та багатьох інших системах застосовується закон, що задається логістичним рівнянням

$$\dot{N} = r\left(1 - \frac{N}{N_c}\right)N, \qquad (1)$$

у якому $\dot{N}$ – (похідна від N), наприклад, швидкість розповсюдження комп'ютерних вірусів; N – кількість комп'ютерних вірусів; N_c – середня кількість комп'ютерних вірусів; r – коефіцієнт народжуваності, кожен вірус може розіслати декілька своїх копій.

Дискретним аналогом логістичного закону є логістичне відображення, яке було застосоване біологом Р. Меєм для аналізу конкретної біологічної ситуації

$$N_{n+1} = r(1 - N_n)N_n, \qquad (2)$$

де N_1, N_2,…, N_m – «можуть відповідати чисельності або біомасі різноманітних видів» [13, с. 22].

Швидкість розповсюдження вірусів пропорційна кількості вірусів і коефіцієнту народжуваності $\dot{N} = rN$. За відсутності перешкод кількість вірусів зростає в геометричній прогресії. Вираз у дужках враховує обмеження ресурсу («запасу поживних речовин»).

Ресурсами для комп'ютерних вірусів є файли в комп'ютерах, де вони можуть розмножуватись. Обмеження ресурсів зменшує коефіцієнт народжуваності і обмежує розповсюдження вірусів. Рівняння (1) описує вихід чисельності вірусів із плином часу на постійне значення, асимптотично наближаючись до максимально можливого значення N_c. За фізичним сенсом розглядаємо лише додатні розв'язки.

Логістичний закон добре описує динаміку зростання популяції комп'ютерних вірусів, коли нема антивірусного захисту, але не враховує всі аспекти боротьби з вірусами за допомогою антивірусних засобів.

На практиці боротьбу з вірусами та іншими інцидентами проводять із певним запізнюванням. Причинами запізнювання можуть бути об'єктивні та суб'єктивні фактори. До об'єктивних факторів запізнювання можна віднести необхідність аналізу нових вірусів та їх модифікацій і розробки та розповсюдження засобів боротьби з ними.

До суб'єктивних факторів можна віднести неправильну розстановку пріоритетів у фінансовій політиці, – на захист інформації треба виділяти кошти, – несвоєчасне виконання запобіжних заходів тощо. Для моделювання системи антивірусного захисту із запізнюванням можна використати рівняння, яке запропонував у 1948 р. Г. Хатчинсон:

$$\dot{N} = r\left(1 - \frac{N(t-\tau)}{N_c}\right)N(t), \tag{3}$$

«Найпростішим дискретним аналогом рівняння Хатчинсона» [13, с. 23] є рівняння

$$N_{n+1} = r(1 - N_{n-1})N_n . \tag{4}$$

Рівняння (3), (4) відрізняється від рівнянь (1), (2) тим, що в ньому введено додатну постійну τ – час запізнювання, яка враховує фактор запізнювання з прийняття заходів щодо установлення засобів антивірусного захисту або оновлення баз даних «синдромів» вірусів. Рівняння (3) описує наступну ситуацію: популяція вірусів розмножується в однорідному середовищі – у комп'ютерній мережі з однаковими комп'ютерами й операційними системами. Є задана кількість поживної речовини – комп'ютерні віруси розмножуються і розповсюджуються через файли із заражених комп'ютерів.

Кількість поживної речовини – число незаражених комп'ютерів поновлюється при зменшенні чисельності комп'ютерних вірусів внаслідок боротьби з вірусами за допомогою антивірусних програм. Коливальний характер епідемії пояснюється наступним. За малої кількості комп'ютерних вірусів та відсутності антивірусів проти них йде активне розмноження вірусів. Через деякий час, із запізнюванням, включаються заходи захисту або для нових вірусів не вистачає ресурсу – незахищених комп'ютерів, де вони можуть розмножуватись. Виникає перенаселеність вірусами. Це призводить до зменшення їх «плодючості» – зменшується коефіцієнт розмноження. Але для меншої кількості вірусів ресурсів уже може вистачати, і їх кількість знову починає зростати. Це може бути через те, що не на всіх вузлах мережі установлені антивірусні заходи, або вони не оновлені тощо. Виникає повторна епідемія. Процес має коливальний характер.

Аналіз показує, що інтенсивність коливань зростає при збільшенні коефіцієнта народжуваності та часу запізнювання τ. При великих значеннях часу запізнювання можуть виникати біфуркації, сингулярності, втрата стабільності.

Райтом [4, п. 9.1.2] було доведено, що рівняння (4) лінійно стійке при

$$r\tau < \pi/2, \tag{5}$$

і дає розв'язання у вигляді коливань навколо стану N_c. При $\tau = 0$ рівняння (4) перетворюється у логістичне рівняння (1). При збільшенні часу запізнювання спостерігається перша біфуркація – режим монотонного зростання або згасання коливань змінюється на режим

згасаючих коливань. При подальшому збільшенні часу запізнювання кількість біфуркацій збільшується і за $\tau \to \infty$ наступає хаос.

У даної моделі є недоліки. У моделі, наприклад, не враховується, що захищені від даного типу вірусу файли більше ним не заражаються, або комп'ютерний вірус модифікується і проти нього ще нема антивірусу, тоді процес починається спочатку.

Інколи «на відміну від класичної фізики, ... у принципово більш складній ситуації може бути не цілком зрозумілим значення математичних символів» [14, розд. 4.3], що вводяться в модель. Крім того, як й інші моделі нелінійної динаміки, вони дають не кількісну, а якісну характеристику головних параметрів динамічних процесів.

Для отримання кількісних характеристик ще треба розробити методику та потужну систему числового моделювання з урахуванням більшого числа факторів. Але результати моделювання, які проведені в даній статті, та здоровий глузд безсумнівно свідчать, що запізнювання з прийняттям рішень щодо захисту інформації (та в інших ситуаціях управління) призводить до збільшення ризиків втрат або збитків.

Звернемо увагу на те, що збільшення ризиків проявляється двічі. Перший раз збитки виникають, коли число інцидентів з інформаційною безпекою збільшується, а захист запізнюється. Другий раз збитки виникають, коли кількість інцидентів падає, а витрати на захист ще залишаються занадто високими.

Все, що було сказано щодо боротьби з комп'ютерними вірусами можна якісно поширити й на деякі інші інциденти з безпекою. Зловмисники «розмножуються» швидше за відсутності контролю та покарання за неправомочні дії. Відсутність контролю та безвідповідальність провокує людей на аморальну поведінку. І навпаки, кількість зловмисників зменшується в умовах контрольованості та справедливості.

Отже, резюмуючи, треба відзначити той фактор, що у сфері захисту інформації залишається досить актуальною проблема уточнення і застосування термінології, зокрема, понять захисту інформації, охорони інформаційних цінностей, безпеки цінностей тощо. Запропоновані в цій статті принципи інтегрованої системи охорони й захисту інформаційних і матеріальних цінностей (ресурсів) в організаціях, установах і підприємствах дозволяє чітко визначити напрями подальших досліджень щодо розробки методів та побудови інтегрованої системи захисту й охорони цінностей, а також створити концептуальні аспекти політики та нормативної бази інтегрованої служби безпеки для підвищення ефективності вибору і формуванні вимог при їх проектуванні та організації. Розроблена модель динаміки процесів у системі захисту цінностей із запізнюванням прийняття управлінських рішень дозволяє формалізувати напрями подальших досліджень щодо розробки нових ефективних систем охорони та захисту ресурсів з використанням інтегральних технологій.

ЛІТЕРАТУРА:

1. Марко Обисо. Развитие международного сотрудничества в области кибербезопасности. Глобальный ответ на глобальный вызов / Marco Obiso, Cebersecuritycoordinator, ITU, Switzerland // Межрегиональный семинар для стран Европы, Азиатско-Тихоокеанского содружества независимых государств (Европа-АТР-СНГ) «Современные методы борьбы с киберпреступностью». – Одеса, Украина, 28-30 марта 2012.
2. Дрозд А. Киберугрозы при использовании мобильного Интернета / Алексей Дрозд // Защита информации. INSIDE. – 2013. – № 1.– С. 42–47.
3. Эшби У.Р. Введение в кибернетику / Эшби У. Р.; [Пер. с англ. Д.Г. Ламути; под ред. В. А. Успенского]. – М.: Изд-во „Иностр. лит.", 1959. – 432.
4. Управление риском; под ред. Г. Г. Малинецкого. – М.: РАН, 2000. – 249 с.
5. Отчет «Лаборатории Касперского»: Java под ударом – эволюция эксплойтов в 2012-2013 гг. – 26с. [Электронный ресурс] – Режим доступа: http://www.securelist.com/ru/analysis/208050816/Otchet_Laboratorii_Kasperskogo_Java_pod_udarom_evolyutsiya_eksploytov_v_2012_2013_gg.

6. Котенко И.В. Интеллектуальные сервисы защиты информации в компьютерных системах и сетях / И.В. Котенко, И.В. Соенко // Защита информации. INSIDE. – 2013. – № 2. – С. 32–41.
7. Казарин О. В. Методология обеспечения проактивной безопасности компьютерных систем / О. В. Казарин, В. Ю. Скиба // Защита информации. INSIDE. – 2013. – № 2. – С. 52–60.
8. Петренко С. А. Вычисления с памятью критически важных информационных систем / [С. А. Петренко, А. Г. Ломако, О. Н. Амельченко, А. В. Зотова] // Защита информации. INSIDE. – 2012. – № 6. – С. 58–69.
9. Волков П. Динамическое управление состоянием безопасности / Павел Волков // Защита информации. INSIDE. – 2013. – № 2. – С. 42–44.
10. Гольдштейн А.Б. SOFTSWITCH / А.Б. Гольдштейн, Б.С. Гольдштейн. – СПб.: БХВ – Санкт-Петербург, 2006. – 368 с.
11. Кучерявый А.Е. От e-России к u-России: тенденции развития электросвязи /А.Е. Кучерявый, Е.А. Кучерявый // Электросвязь. – 2005. - № 5. – С. 10.
12. Любошинский М. К вопросу оценки информации как ресурса / Михаил Любощинский // SciTecLibrary.ru, 2012. – 3 с. [Электронный ресурс] – Режим доступа: http://www.sciteclibrary.ru/rus/catalog/pages/12450.html.
13. Малинецкий Г.Г. Математические основы синергетики. Хаос, структура, вычислительный експеримент / Малинецкий Г.Г. – М.: КомКнига, 2005. – 312 с.
14. Тутубалин В.Н. Математическое моделирование в экологии: Историко-методологический анализ / [В. Н Тутубалин, Ю. М. Барабашева, А. А. Григорян, Г. Н Девяткова, Е. Г. Угер]. – М.: «Языки рус. культ.», 1999. – 236 с.

REFERENCES:

1. Obiso M. (2012). Development of international cooperation in cybersecurity. A global response to a global challenge. – 2012.
2. Drozd A. (2013). Cyber threats when using the mobile Internet / Information Security INSIDE. – 2013. – № 1. – P. 42–47.
3. Ashby W.R.(1959). Introduction to cybernetics. Publishing House of the "Foreign Literature”, 1959. – P. 432.
4. Malinetskiy G.G. ed. (2000). Risk management. RAN, – 2000. – P. 249.
5. Report on "Kaspersky Labs»: Java under attack - the evolution of exploits in 2012-2013. – 26 sec. http://www.securelist.com/ru/analysis/208050816/Otchet_Laboratorii_Kasperskogo_Java_pod_udarom_evolyutsiya_eksploytov_v_2012_2013_gg.
6. Kotenko I.V , Soenko I.V.(2013). Intellectual services of information security in computer systems and networks / Information Security. INSIDE. – 2013. – № 2. – P. 32– 41.
7. Casarin O.V., Skiba V.Y. (2013). Methodology provide proactive security of computer systems / Information Security. INSIDE. – 2013. - № 2. – p. 52– 60.
8. Petrenko S.A, Lomako A.G, Amel'chenko O.N, Zotov A.V. (2012). Computing with Memory-critical information systems / Information Security. INSIDE. – 2012. - № 6. – P. 58– 69.
9. Volkov P. (2013). Dynamic control of the safety / Information Security. INSIDE – 2013. – № 2. – P. 42 – 44.
10. Goldstein A.B., Goldstein B.S. (2006). SOFTSWITCH. – BHV, 2006. – P. 368.
11. Kucheryavyy A.E., E.A Kucheryavyy A.E. (2005). By e-Russian to the u-Russia: Trends Telecommunication / Magazine “Telecommunications”. – 2005. – № 5. – P. 10.
12. On assessment information as a resource. http://www.sciteclibrary.ru/rus/catalog/pages/12450.html.
13. Malinetskii G.G.(2005). Mathematical Foundations of Synergetics. Chaos, structure, computational eksperiment / Malinetskii G.G. – KomKniga, 2005. – P.312.
14. Tutubalin V.N., Barabashev Y.M., Grigoryan A.A., Devyatkova G.N., Uher E.G. (1999). Mathematical modeling in ecology: Historical and methodological analysis / Languages Russian culture, – 1999. – P. 236.