УДК 004.056
DOI: 10.31673/2409-7292.2018.031622

Шуклін Г.В., Барабаш О.В.

ТЕОРЕТИЧНІ ЗАСАДИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ НА ФОНДОВОМУ РИНКУ: МЕХАНІЗМИ,МЕТОДИ,ІНСТРУМЕНТИ

В даній статті досліджено поняття «державного регулювання кібербезпеки», наведено власне визначення державного регулювання кібербезпеки, яке необхідно розглядати як систему, яка здійснює цілеспрямований вплив органів державної влади на рівень розвитку інформаційно-телекомунікаційних систем, з'ясовано зміст поняття «державне регулювання кібербезпеки фондового ринку», визначено механізм, методи та інструменти. Запропоновано математичну модель прогнозування кібернетичних атак.

Ключові слова: фондовий ринок,загрози,державне регулювання,запізнення,кібербезпека

Постановка завдання. Однією із складових економіки держави є фондовий ринок. Прозоре його функціонування дає можливість державі створювати відповідні умови, коли фізичні особи мають можливість вкладати свої накопичення не в фінансові установи (банки, трасти, тощо), а в цінні папери, емісія яких здійснюється як крупними приватними компаніями так і державою. Також, фондовий ринок створює умови для залучення інвестицій, що сприяє позитивному розвитку економіки держави і надходженню додаткових коштів до бюджету.

Проте, на теперішній час торги на фондовому ринку здійснюються на спеціалізованих електронних майданчиках в віддаленому доступі. Саме, завдяки цьому, існування в інформаційному просторі віртуальної грошової одиниці для кіберзлочинців існує можливість створювати різноманітні кримінальні схеми фінансових операцій. З однієї сторони, вони здійснюють «відмивання» грошей, отриманих злочинним шляхом, що не дає можливості надходження коштів до державного бюджету у вигляді податків, а з іншої, вони присвоюють собі власність третіх осіб, які здійснюють прозорі торги на фондовому ринку. Тому, створення віртуальних грошей призвело до нових проблем в кіберпросторі.

Фахівцями з кібербезпеки Ю.В. Борсуковським, В.Л. Бурячком, В.Ю.Борсуковською ставляться дві основні проблеми, пов'язаними з віртуальними грошима. Перша проблема полягає в перетику віртуальних біткоінів в матеріальний простір, що стає додатковим стимулюючим фактором для зростання злочинності в кіберпросторі. Другою проблемою в кіберпросторі є реалізація кіберстратегій на рівні державних політик [1]. Ці дві проблеми створюють реальну небезпеку для економіки держави і одним з об'єктів реалізації кіберзлочинності стає фондовий ринок.

Виклад основного матеріалу. В проекті концепції інформаційної безпеки України дається означення трьох понять, а саме, ***забезпечення інформаційної безпеки, кібернетичної безпеки*** і ***кібернетичного простору*** [2]. Вони визначають загальне уявлення про інформаційну безпеку і є основними складовими в регулюванні кібербезпекою.

Слід зазначити, що проблема державного регулювання кібербезпекою є предметом досліджень багатьох фахівців сучасності.

Так, О.К. Юдін визначає, що однією з загроз інформаційній безпеці держави є перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин. [3]

На нашу думку, державне регулювання кібербезпеки необхідно розглядати як систему, яка здійснює цілеспрямований вплив органів державної влади на рівень розвитку інформаційно-телекомунікаційних систем та містить наступні складові: зміст регулювання; предмет, об'єкти та суб'єкти регулювання; завдання регулювального впливу; механізм впливу держави на стан інформаційної захищеності; результати державного регулювання кібербезпеки.

Важливим науковим завданням є з'ясування змісту поняття «державне регулювання кібербезпеки фондового ринку». Беручи до уваги той факт, що досліджувана категорія є складовою частиною системи державного регулювання кіберпбезпеки, доцільно розпочати із вивчення та критичної оцінки наукових поглядів.

На основі аналізу сучасних наукових поглядів та власної позиції щодо сутності фондового ринку та державного регулювання кібербезпекою визначено сутнісні характеристики державного регулювання кібербезпеки фондового ринку, а саме:

- останнє охоплює відносини, які виникають між інформаційно-телекомунікаційною системою та державою;
- до сфери впливу державного регулювання залучені всі інформаційно - телекомунікаційні системи, функції яких є протидія кіберзлочинності, всі інформаційно-телекомунікаційні системи суб'єктів фондового ринку, та забезпечується здійснення ними своєї діяльності відповідно до встановлених правил;
- є елементом загальної системи управління державою та закладає основи для формування нових конкурентних переваг національної економіки;
- є наукою про процеси та явища, що відбуваються у сфері цілеспрямованого впливу органів державної влади на рівень розвитку інформаційної захищеності фондового ринку;
- реалізація державного регулювання забезпечується системою органів державної законодавчої, виконавчої та судової влади, які відповідно до законодавства наділені повноваженями у сфері регулюючого впливу на кібербезпеку фондового ринку, а також науково-дослідними установами;
- відносини у сфері державного регулювання кібербезпекою фондового ринку базуються на закріплених законами та іншими нормативно-правовими актами юридичних нормах;
- становить циклічний процес прийняття рішень у сфері цілеспрямованого впливу на кібербезпеку фондового ринку.

Враховуючи вищезазначене, можна стверджувати, що державне регулювання кібербезпеки фондового ринку є наука, система та процес.

Таким чином, державне регулювання кібербезпеки фондового ринку як наука є сукупністю знань та наукових поглядів на явища та процеси, що об'єктивно відбуваються у кіберпросторі між державою та фондовим ринком у процесі їх взаємодії.

Як систему державне регулювання кібербезпекою фондового ринку необхідно розглядати як динамічне цілісне середовище, що дозволяє здійснювати вплив на інформаційно-телекомунікаційні структури фондового ринку та їх взаємодію.

Як приклад в необхідності цього, можна згадати 27 червня 2017 року, коли в інформаційно-комунікаційну систему Української фондової біржі та на фондовій біржі ПФТС було запущено вірус Petya, що призвело до того, що фондовий ринок України «ліг». В результаті учасники фондового ринку і держава в тому числі понесла величезні збитки. Якщо б з боку держави здійснювалось відповідне регулювання кібербезпеки в першу чергу Службою безпеки України, то такого можливо і не сталося.

Систему державного регулювання кібербезпеки доцільно аналізувати з економіко-правової та організаційної точок зору. З економіко-правової точки зору, державне регулювання кібербезпеки – це сукупність норм, методів та правил організації відносин між державою та фондовим ринком з метою забезпечення висхідного поступу соціально-економічного розвитку країни та її інтеграції у світовий економічний простір.

До функцій державного регулювання кібербезпеки фондового ринку можна зарахувати такі:

- створення системи підтримки прийняття рішень в процесі відновлення та забезпечення комплексної захищеності інформаційних систем на фондовому ринку. Проектування таких систем запропоновано С.В.Толюпою [4];

- оцінка ефективності системи захисту інформації на фондовому ринку. Такі методи запропоновані Р.В.Грищуком [5], В.О.Хорошко і Ю.Є. Хохлачовою [6];
- управління, в тому числі, оптимальне управління в системах захисту інформації на фондовому ринку. Запропоновано Р.В.Грищуком, В.О. Хорошко та Ю.Є. Хохлачовою [7], також Г.В.Шукліним та О.П.Коломійчуком [8];
- забезпечення інформаційного контролю над рухом віртуальних грошових одиниць при використанні їх на торгах на фондовому ринку, та інші функції.

Досвід країн з розвиненою економікою показує, що фондовий ринок, на відміну від інших ринків (зокрема, товарного або валютного), є одним із найбільш регульованих та регламентованих. Основна причина в тому, що неврегульований рух капіталів вже багато разів в історії різних країн завдав значної шкоди їх фінансовим системам.

Система регулювання кібербезпеки фондового ринку в більшості країн світу має два рівні: саморегулювання кібербезпеки професійних учасників та державного регулювання. З них історично першим виникло саморегулювання, що здійснювалося фондовими біржами, які створювали стандартні правила гри стосовно окремих груп учасників фондового ринку, які працювали для всіх суб'єктів [9].

Сутність державного регулювання кібербезпекою фондового ринку полягає у реалізації комплексу заходів щодо нагляду за інформаційно-комунікаційними системами, які використовуються при здійснені торгів цінними паперами та фінансовими інструментами, здійснення контролю за дотриманням стандартів в сфері інформаційної безпеки, виявлення кібершпигунів, які намагаються здійснювати зломи з метою привласнення активів та володіння комерційними тайнами, а також забезпечення впливу держави на кіберпростір фондового ринку з метою досягнення відповідності до загальнодержавних інтересів та стратегії економічного розвитку.

Державне регулювання кібербезпекою фондового ринку здійснюється для досягнення чітко визначених цілей (рис.1).

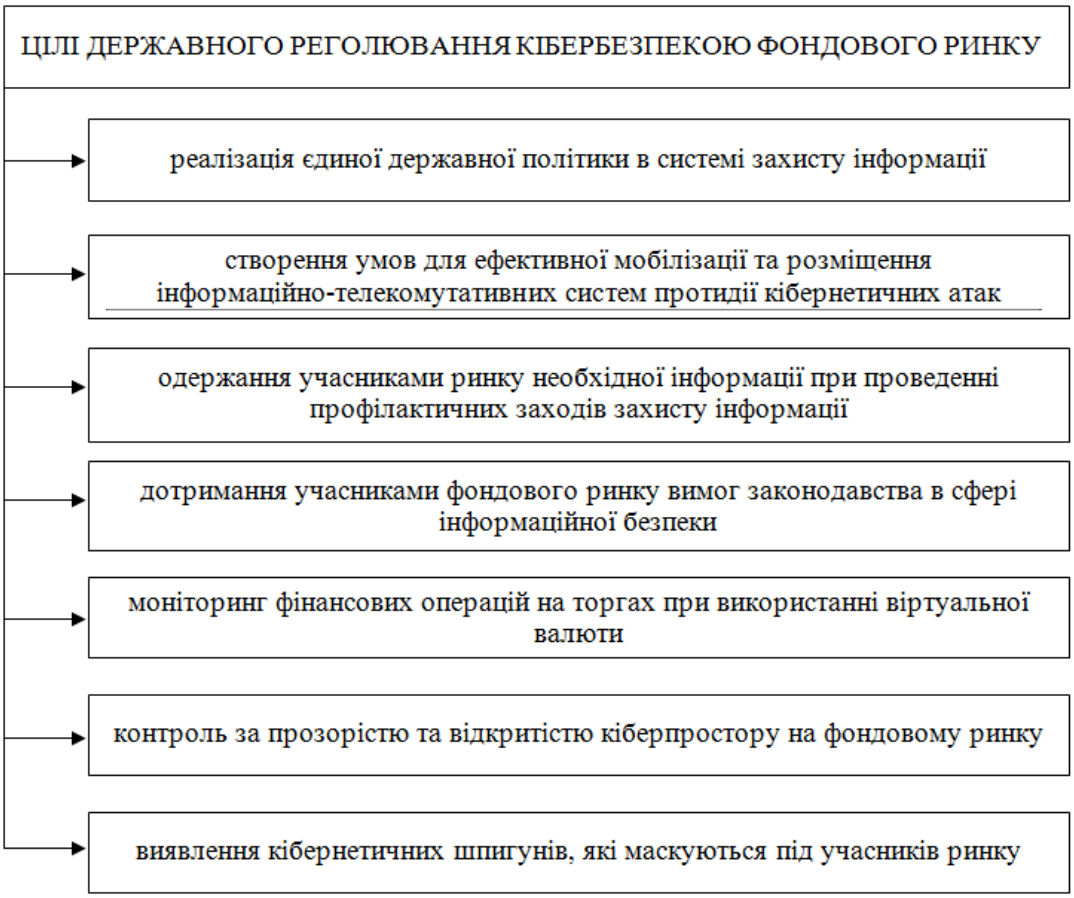

Рис.1. Основні цілі державного регулювання кібербезпеки фондового ринку

Доцільність здійснення державного регулювання кіберпростору фондового ринку обґрунтована наступними чинниками:

- потребою у регулювання взаємовідносин різних учасників ринку з метою узгодження їх виходу в кібернетичний простір фондового ринку, а також координації їх діяльності;
- необхідністю створення міцної законодавчої бази в області інформаційної безпеки, здійснення контрольних заходів задля забезпечення стандартизації інформаційно-телекомунікаційних систем, функціонування яких направлено на захист кібернетичного простору фондового ринку;
- постійною присутністю складності захисту інформації, пов'язаною зі швидкістю розвитку інформаційних технологій.

Для здійснення якісного регулювання кібербезпекою фондового ринку з боку держави необхідним є відповідний математичний апарат за допомогою якого розвивається інформаційно – телекомунікаційна система, що забезпечує досягненню відповідної мети. Враховуючи відмінність фондового ринку від інших об'єктів кіберзлочинних інтересів, слід створювати такі математичні моделі, які давали можливість захищати відповідний об'єкт в залежності від його особливостей.

Особливу увагу при створенні таких моделей заслуговує робота Р.В. Грищука, в якій застосовується диференціально-ігровий метод, щодо регулювання та оцінки ефективності систем захисту інформації [5]. Також, В.О. Хорошко і О.М.Чернишев використовують алгебраїчно-статистичний підхід виявлення атак для засобів моніторингу інформації [10]. Ефективними є генетичні алгоритми при розв'язуванні задач інформаційної безпеки [11].

В роботі [10] пропонується алгоритм виявлення атак, в якому для формування ймовірності в системі обробки інформації (СОІ) використовується розширений сеансовий вектор $X = \{x_1, x_2, \dots, x_n\}$, що являє собою лічильник факторів різноманітних загроз безпеки x_i, що зафіксовані засобами збору інформації і перевірки стану СОІ чи мереж.

При формуванні даного вектору на фондовому ринку слід враховувати фактори загроз, які виникали до поточного моменту часу і на основі аналізу здійснювати прогноз майбутніх можливих загроз. Для вирішення даного завдання, авторами пропонується математична модель у вигляді диференціального рівняння з чистим запізненням, яке має наступний вигляд

$$\dot{x}(t) = Ax(t-\tau)\ ,\ x(t) \in R^n,\ t \geq 0,\ \tau > 0,\ \ x(t) \equiv \varphi(t)\ ,-\tau \leq t \leq 0 \tag{1}$$

Розв"язок $x(t)$-фактор загроз в момент часу t, системи (1), що задовольняє початковим умовам $x(t) \equiv \varphi(t)\ ,-\tau \leq t \leq 0$, де $\varphi(t)-$ неперервно диференційована векторна функція, побудована на базі закону розподілу різноманітних загроз протягом попереднього проміжку часу τ, має вигляд

$$x(t) = e_\tau^{At}\varphi(-\tau) + \int_{-\tau}^{0} e_\tau^{A(t-\tau-s)}\varphi'(s)\ ds\,, \tag{2}$$

де

$$e_\tau^{At} = \begin{cases} \theta\ , & -\infty < t < -\tau \\ I\ , & -\tau \leq t < 0 \\ I + A\dfrac{t}{1!} + A^2\dfrac{(t-\tau)^2}{2!} + \cdots + A^k\dfrac{[t-(k-\tau)]^k}{k!}, & (k-1)\tau \leq t < k\tau \end{cases} \tag{3}$$

Векторна функція (3) отримала назву запізнюючого експоненціала [12]. Квадратна матриця A, уявляє собою матрицею інформаційного впливу [8], який є загрозою кібернетичного простору, чисельні елементи якої формуються експертами інформаційної безпеки, які є аналітиками кібернетичного простору на фондовому ринку.

Приклад. Протягом 2017 року в кібернетичний простір Української фондової біржі відбувався фактор загроз $x_1(t)$- намагання запуску вірусу в електронну торгівельну платформу, залежність якого від часу на базі побудованого закону розподілу, мав вигляд

$$x_1(t) = t^2 + 2 \ .$$

В той самий час був ще один фактор загроз $x_2(t)$ - спроба певними учасниками фондового ринку, використовуючи віртуальну валюту, вивести не законним шляхом кошти за межі України, через операції з цінними паперами на фондовій біржі. Аналогічним чином, було отримано, що

$$x_2(t) = t^3 \ .$$

Тоді, якщо прийняти $\tau = 1$ рік, то на 01.01.2018 року, векторна функція $\varphi(t)$ має вигляд

$$\varphi(t) = \begin{pmatrix} t^2 + 2 \\ t^3 \end{pmatrix} \ .$$

При цьому, матриця інформаційного впливу мала наступний вид $A = \begin{pmatrix} 0{,}3 & 0{,}7 \\ 0{,}5 & 0{,}5 \end{pmatrix}$. Тоді, система (1) прийме вигляд

$$\begin{cases} \dot{x_1}(t) = 0.3x_1(t-1) + 0.7x_2(t) \\ \dot{x_2}(t) = 0.5x_1(t-1) + 0.5x_2(t-1) \end{cases}, \quad \begin{cases} x_1(t) = t^2 + 2 \\ x_2(t) = t^3 \end{cases} \text{ при } -1 < t < 0 \ . \tag{4}$$

Функція (3) має структуру $e_\tau^{At} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, при $-1 < t < 0$ і $e_\tau^{At} = \begin{pmatrix} 1 + 0{,}3t & 0{,}7t \\ 0{,}5t & 1 + 0{,}5t \end{pmatrix}$, при $0 < t < 1$.

І розв'язок (2) системи (4) визначається наступним чином

$$\begin{cases} x_1(t) = 2{,}1t^3 + 2{,}3t + 1{,}695 \\ x_2(t) = 1{,}5t^3 + 3t^2 + 0{,}8t + 1{,}045 \end{cases}, \text{ при } 0 < t < 1. \tag{5}$$

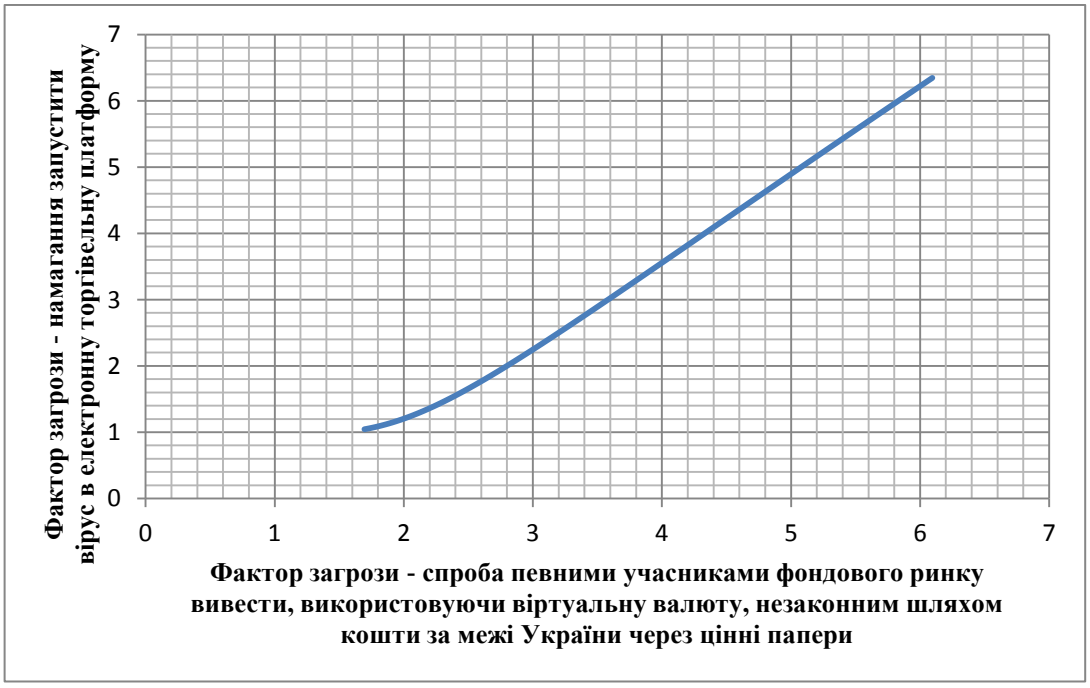

Рис. 2. Взаємозалежність двох факторів загроз

На рисунку 2 побудовано залежність фактору загроз $x_1(t)$ від фактору загроз $x_2(t)$, залежності від часу яких представлено системою (5) протягом 2017 року. З графіка видно, що ці два фактори мають пряму залежність один від одного. Цей факт показує, що проблему кібернетичних загроз необхідно розглядати комплексно, тобто захист необхідно здійснювати одночасно по всім напрямкам.

Висновки. Кібернетична безпека фондового ринку є однією із складових інформаційної безпеки держави. Функціонування відповідного механізму державного регулювання кібербезпеки фондового ринку має спрямованість на забезпечення таких результатів:

1. Підвищення повноважень органів державного регулювання кібербезпеки фондового ринку з метою більш поглибленого аналізу вразливості інформаційно-комунікаційних систем, що забезпечують інформаційну безпеку.
2. Посилення контролю за адекватністю фінансових ресурсів, обсягом і характером операцій, які здійснюють учасники фондового ринку з використанням віртуальної валюти, шляхом уведення більш жорстких санкцій за порушення чинного законодавства.
3. Забезпечення відкритості інформаційного забезпечення фондового ринку шляхом оприлюднення всієї суттєвої інформації щодо здійсню вальних операцій.
4. Провадження цілісної, підпорядкованої взаємодії органів державного регулювання інформаційної безпеки фондового ринку на основі створення єдиної інформаційної бази, забезпеченої можливостями вільного доступу будь-якого з відповідних державних органів, що дозволить оптимізувати процеси взаємодії, спільної роботи і комплексної оцінки інформаційної безпеки на макрорівні.
5. Використання систем диференціальних рівнянь з запізненням, як математичну модель прогнозування кібернетичних атак, дають можливість не тільки спрогнозувати періоди атак, а також встановити взаємозв'язок між факторами, які цьому сприяють.
6. Враховуючи ефект запізнення, ми маємо змогу отримувати нову додаткову інформацію, яка не враховувалась раніше.

Список використаних джерел

1. Борсуковський Ю.В. Базові напрямки забезпечення кібербезпеки державного та приватного секторів / Ю.В. Борсуковський, В.Л. Бурячок, В.Ю. Борсуковська // Сучасний захист інформації. - №2(30), 2017.- с.85-89.
2. Проект Концепції інформаційної безпеки України : [Електронний ресурс] / Офіційний сайт Міністерства інформаційної політики України. – Режим доступу: http://www.mip.gov.ua/documents/30.html (дата звернення 25.07.2018). - Назва з екрану.
3. Юдін О.К. Інформаційна безпека держави : навч. посіб./ О.К. Юдін, В.М. Богуш. – Харків: Консум, 2004. – 508 с.
4. Тюлюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защиты информационных систем / С.В. Тюлюпа // Сучасний захист інформації. - №4, 2012. – с.69-74.
5. Грищук Р.В. Диференціально-ігровий метод оцінювання ефективності систем захисту інформації / Р.В.Грищук // Сучасний захист інформації. - №1,2012. – С 40-44.
6. Хорошко В.О. Оцінка захищеності інформаційних систем / В.О.Хорошко, Ю.Є. Хохлачова. // Сучасний захист інформації №4,2012.- с 50-89.
7. Грищук Р.В. Використання диференціальних ігор для оптимізації управління в системах захисту інформації /Грищук Р.В., Хорошко В.О. , Хохлачова Ю.Є. // Сучасний захист інформації №2,2012.- с 21-26.
8. Шуклін Г.В.Забезпечення інформаційної безпеки на фондовій біржі за допомогою методів теорії керування / О.П. Коломійчук, Г.В. Шуклін // Моделювання та інформаційні системи в економіці. Збірник наукових праць. – 2015. – Випуск 90. – С.208-215.
9. Ahentstvo z rozvytku infrastruktury fondovoho rynku Ukrayiny.Vlasnyky krupnykh paketiv aktsiy PrAT «Fondova birzha PFTS». (2010). Retrieved from: URL:http://smida.gov.ua/db/owners/21672206/2010/2.
10. Хорошко В.О. Алгоритм виявлення атак для засобів моніторингу інформації / В.О. Хорошко, О.М. Чернишев // Сучасний захист інформації. - №1, 2012. – с. 49-56.

11. Невойт Я.В. Влияние генетических алгоритмов на эффективность решения задач по информационной безопасности / Невойт Я.В., Хорошко В.А.// Сучасний захист інформації №2,2012.- с 58-64.

12. Д.Я.Хусаінов. Керування в системах з чистим запізненням.// Д.Я. Хусаінов, Г.В. Шуклін. Вісник Київського Університету, випуск №1, 2002р. С. 267-276.

13. Грищук Р.В. Основи кібернетичної безпеки: монографія / Р.В. Грищук, Ю.Г. Даник; під заг. Ред. проф. Ю.Г. Даника.- Житомир: ЖВІ ім. С.П.Корольова, 2016.- 636 с.

14. Доктрина інформаційної безпеки України (затверджена указом Президента України №47/2017 від 25 лютого 2017 року) : [Електронний ресурс] / Офіційне представництво Президента України. – режим доступу: http://www.president.gov.ua/documents/472017-21374 (дата звернення 25.07.2018). - Назва з екрану.

15. Шуклин Г.В. Методы построения правил принятия инвестиционных решений на фондовом рынке [Електронний ресурс] / Г.В.Шуклін // Соціально-економічні проблеми і держава. – 2014. – Випуск 1(10). – Режим доступу до журналу: http: // sepd.tntu.edu.ua/images/stories/pdf/2014/14sqvnfr.pdf.

Надійшла: 16.06.2018 Рецензент: к.т.н. Довбешко С.В.