УДК 004.056 к.т.н. **Лахно В.А.** (СУНУ ім. В.Даля)

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ ДИСПЕТЧЕРСЬКОГО УПРАВЛІННЯ І ЗБИРАННЯ ДАНИХ

У статті запропоновано алгоритм моделювання процесу прийняття рішення щодо вибору оптимальної стратегії управління інвестиційним проектуванням СЗІ для господарюючого суб'єкта на транспорті.

Ключові слова: захист інформації, інформаційна безпека, моделювання процесу прийняття рішення.

В статье предложен алгоритм моделирования процесса принятия решения по выбору оптимальной стратегии управления инвестиционным проектированием систем защиты информации для хозяйствующего субъекта на транспорте.

Ключевые слова: защита информации, информационная безопасность, моделирование процесса принятия решений.

In the article the algorithm of modeling of process of decision-making at the choice of optimum strategy of management by investment design of systems of information security for the managing subject on transport is offered.

Keywords: information security, information security, decision-making process, modeling.

Постановка проблеми. Диспетчерське управління і збір даних (SCADA Supervisory Control And Data Acquisition) є основним і на даний момент залишається найбільш перспективним методом автоматизованого управління складними динамічними системами (процесами) в життєво важливих і критичних з точки зору безпеки і надійності областях. Саме на принципах диспетчерського управління будуються великі автоматизовані інформаційні системи (АІС) в промисловості, енергетиці, на транспорті, в космічній і військовій областях, в різних державних структурах. Наприклад, "Укрзалізниця" завершує роботу над створенням електронної карти залізниць України. За допомогою спеціальних координат визначатимуться станції, світлофори, переїзди і так далі Відповідна інформація в майбутньому надаватиметься пасажирам, зустрічаючим, вантажоодержувачам, операторам і іншим споживачам. За місцем знаходження локомотива визначатиметься весь склад поїзда: він вантажний або пасажирський, скільки вагонів, куди прямує, який вантаж перевозить і так далі АІС враховуватиме пробіг вагонів, локомотивів, навантаження на колії і ін.

Розслідування і аналіз більшості аварій і подій в авіації, наземному і водному транспорті, промисловості і енергетиці, частина з яких привела до катастрофічних наслідків, показали, що, якщо в 60-х роках минулого сторіччя помилка людини була первинною причиною лише 20% інцидентів (80%, відповідно, за технологічними несправностями і відмовами), то на початку 21-го століття частка людського чинника зросла до 80%, причому, у зв'язку з постійним вдосконаленням інформаційних технологій і підвищенням надійності комунікаційного устаткування і машин, частка ця може ще зрости [1, 2, 3]. Подальший розвиток сучасних систем диспетчерського управління і збору даних не можливий без вирішення проблем їх безпеки, зокрема інформаційних [3].

Головною метою будь-якої системи інформаційної безпеки (ІБ) є забезпечення стійкого функціонування об'єкту, запобігання загроз його безпеки, захист законних інтересів замовника від протиправних посягань, недопущення розкрадання фінансових коштів, розголошування, втрати, спотворення і знищення службової інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об'єкту.

Про серйозність проблеми говорить хоч би такий факт - одна людина за незначний час в змозі повністю паралізувати об'єкт інформаційної атаки, якщо вона має доступ до даних АІС. Для цього досить ввести в програмне забезпечення АІС всього декілька десятків рядків

коду програми-вірусу. Якщо дана система не матиме спеціальних засобів захисту, то це їй загрожуватиме як мінімум суттєвими економічними втратами.

Мета роботи полягає в отриманні алгоритму моделювання процесу прийняття рішення щодо вибору оптимальної стратегії управління інвестиційним проектуванням СЗІ для господарюючого суб'єкта на транспорті.

Огляд попередніх досліджень. Як показує досвід експлуатації АІС в різних областях, гарантоване стовідсоткове забезпечення інформаційної безпеки справа дорога і не завжди доцільна, оскільки:

1) навіть найдосконаліша на сьогодні система захисту інформації (СЗІ) не може протидіяти загрозам, які можуть виникнути в подальшому.

Ось лише декілька прикладів за останні три роки. На початку 2010 року в пресі [4] обговорювався абсолютно новий тип загроз конфіденційності інформації, що зберігається на мобільних пристроях співробітників компанії. Той, що атакує теоретично може дістати доступ до пристрою, підключеному до мережі, і виконати на нім довільний код або викрасти конфіденційну інформацію. Фахівці компанії Juniper Networks стверджують, що відкрили новий тип хакерських атак, яким піддаються різноманітні пристрої, зокрема смартфони, комунікатори (вельми популярні у вищого менеджменту будь-якої компанії), кишенькові комп'ютери і ін.

Про те, що початок кібервійн не за горами, свідчать промислові віруси, направлені насамперед на підрив роботи промислових і транспортних систем.

У січні ізраїльські хакери блокували сайти фондових бірж Саудівської Аравії і ОАЕ. Ці дії були нібито ударом у відповідь на атаки саудівських хакерів по ізраїльських порталах - Тель-авівській біржі і ізраїльській національній авіакомпанії "Ель Аль". В кінці травня 2012 р. наслідки кіберрозборок на Близькому Сході сталі помітніші. У Ірані вірус під кодовою назвою Flame вразив міністерство нафти і нафтові термінали країни. Поширення вірусу було зупинено, але є підстави вважати, що він потрапив в комп'ютерну мережу відомства багато місяців тому і виконав головне завдання зі збору і відправки інформації [5]. Як показав подальший аналіз [5], Flame не є механізмом створення економічної вигоди, а може служити тільки як кіберзброя.

Більшість експертів сходяться на думці, що настільки великий і могутній вірус міг бути створений тільки за підтримки якоїсь держави. Більш того, незважаючи на відсутність явних аналогій з вірусами Stuxnet [6] (був спрямований на зрив ядерної програми Ірану) і Duqu [7] (вважається за допоміжний інструмент, споріднений зі Stuxnet), є ряд ознак, що вказують на те, що вірус був створений іншою командою розробників, але в один період і в одній організації. Зокрема, експерти знайшли у вірусі Flame використання тих же вразливостей, які 5-6 років тому застосовувалися для поширення вірусів Stuxnet і Duqu через USB-флешки (за допомогою механізму авто запуску і через файли ярликів .LNK) і по локальних мережах. Хоча всі ці проблеми давно виправлені, фахівці досі гадають, як саме вірус виконує початкове зараження комп'ютерів – є докази, що він може бути присутнім в операційній системі Windows 7 з усіма актуальними оновленнями і антивірусами. При цьому, наскільки відомо, механізм автоматичного розповсюдження і зараження у вірусі відключений.

2) вартість комплексного захисту може виявитися значно вище, ніж вартість інформаційних ресурсів, які потребують захисту.

Основний матеріал статті. На даний момент в розвинених зарубіжних країнах спостерігається справжній підйом по впровадженню нових і модернізації існуючих автоматизованих систем управління в різних галузях економіки. Характерно, що в індустріальній сфері (в оброблювальній і добувній промисловості, енергетиці і ін.) найчастіше згадується саме модернізація існуючих виробництв SCADA-системами нового покоління [8]. Велика увага приділяється модернізації виробництв, які представляють собою екологічну небезпеку для навколишнього середовища (хімічні та ядерні підприємства), а також тих, що грають ключову роль в життєзабезпеченні країни, зокрема, транспорт. З

початку 90-х років в США почалися інтенсивні дослідження і розробки в області створення автоматизованих систем управління наземним транспортом ATMS (Advanced Traffic Management System).

Велику допомогу в побудові ефективної системи інформаційної безпеки (СІБ) можуть надати методи математичного моделювання. По-перше, саме за їх допомогою можна наочно довести менеджерам, що вкладення коштів в СЗІ дійсно зекономить гроші компанії (недооцінка необхідності ІБ менеджерами компанії є в більшості випадків основною перешкодою в її розвитку). По-друге, в умовах обмеженості ресурсів, відпущених на СЗІ, за допомогою цих методів можна вибрати найбільш оптимальний комплекс засобів захисту, а також змоделювати, наскільки створена СЗІ виявиться ефективною в боротьбі проти найбільш поширених загроз.

В процесі формування моделі оптимізації комплексу засобів захисту інформації була розроблена методика послідовності фінансового прогнозування витрат компанії на СЗІ, яку можна представити в наступному вигляді: формування прогнозу прибутку господарюючого суб'єкта; формування прогнозу змінних і постійних витрат господарюючого суб'єкта; формування прогнозу інвестицій в СЗІ, необхідних для досягнення прогнозованих прибутків; розрахунок можливих обсягів внутрішнього фінансування; розрахунок потреб у зовнішньому фінансуванні (позиковому капіталі); пошук джерел зовнішнього фінансування з урахуванням формування раціональної структури капіталу.

На підставі аналізу методів прогнозування результатів інвестиційного проектування, і використовуючи раніше викладену модель оптимізації витрат на комплекс СЗІ, і управління інформаційною безпекою [3,9] на транспорті, в роботі пропонується економетрична модель вибору оптимальної стратегії управління інвестиційним проектуванням СЗІ для господарюючого суб'єкта, загальна схема якої складається з реалізації таких основних етапів.

1. Ґрунтуючись на даних системного аналізу, визначаються можливі стратегії розвитку господарюючого суб'єкта, його інфокомунікаціної структури і завдань забезпечення інформаційної безпеки.

2. Для визначення прогнозних обсягів послуг (товарів), використовується метод множинного регресійного аналізу. На основі залежності функції (обсяг реалізації) від факторів (собівартість, ціна реалізації, індекс споживчих цін, витрати на рекламу і ін.), будується модель множинної регресії, яка використовується як прогнозна модель у вигляді:

$$U = A + a_1 \times x_1 + a_2 \times x_2 + a_3 \times x_3 + ... + a_n \times x_n ,$$

де U – прогнозний обсяг послуг (продажів) компанії; x_j, $j \in \overline{1,m}$ – незалежні змінні (наприклад, витрати на рекламу і ін.); A – константа рівняння регресії; a_j , $j \in \overline{1,m}$ – коефіцієнти рівняння регресії.

3. Формуються прогнозні значення обсягів реалізації послуг (продажів) на наступний період часу для платіжної матриці шляхом варіювання значень змінних у відповідності з безліччю пропонованих стратегій $C = \{C_k\}$ (зокрема стратегій, що передбачають розвиток інфокомунікаційної структури компанії і відповідних засобів захисту інформації), $k \in \overline{1,q}$, де q - кількість стратегій, і значеннями можливих станів ринкової кон'юнктури X_j, $j \in \overline{1,m}$, де m - кількість станів ринкової кон'юнктури; формується матриця обсягів реалізації послуг (продажів) - $U = \|u_{kj}\|$, $k \in \overline{1,q}$, $j \in \overline{1,m}$. В якості k-*ої* допустимої стратегії управління C_k ($k \in \overline{1,q}$) пропонується розглядати сукупність дій господарюючого суб'єкта, які характеризуються рівнем витрат, певною збутовою і ціновою політикою, бюджетом реклами і іншими внутрішніми чинниками.

В якості стану ринкової кон'юнктури розглядаються різні поєднання зовнішніх, незалежних від господарюючого суб'єкта чинників (ємкість ринку, інфляція, питання ІБ і так далі), тобто - X_j – це *j-е* прогнозне значення стану ринку, що характеризується ємкістю ринку транспортних послуг, певним рівнем інфляції та іншими, незалежними від господарюючого суб'єкта, зовнішніми чинниками.

Наприклад, в процесі проведення аналізу за стратегією забезпечення захисту інформації, спочатку, з урахуванням конкретної ситуації на підприємстві, складається список його слабких і сильних сторін, що характеризує стан внутрішнього середовища підприємства, яке має декілька складових. Кожна зі складових внутрішнього середовища включає сукупність ключових процесів і структурних елементів об'єкту аналізу, що визначають в сукупності потенціал і можливості, які має в своєму розпорядженні підприємство (компанія, галузь). Приклад аналізу сильних і слабких сторін підприємства приведений в таблиці 1.

Таблиця 1

Приклад аналізу сильних і слабких сторін транспортної компанії

Складові внутрішнього середовища	Ефективність складових внутрішнього середовища				Важливість		
	Дуже сильна	Сильна	Нейтральна	Слабка	Висока	Середня	Низька
1. Маркетинг							
1.1.Репутація підприємства	+				+		
1.2. Ринкова частка		+			+		
1.3. Якість послуг (зокрема інформаційних)	+		+		+		
1.4. Витрати виробництва та ін.			+			+	
2. Фінансовий аналіз							
2.1. Рівень прибутковості				+	+		
2.2. Фінансова стабільність та ін.		+	+		+		
3. Організація і кадри							
3.1. Підприємницька орієнтація				+		+	
3.2. Кваліфікація персоналу та ін.				+		+	
.....							
4. Інформаційні технології і системи							
4.1. Рівень застосування ІТ і ІС		+			+	+	
4.2. Інтеграція з глобальними мережами та ін.			+				+
.....							
5. Інформаційна безпека							
5.1. Наявність спеціальних структур з питань ІБ			+			+	
5.2. Постійний або періодичний аудит ІБ та ін.		+	+			+	
.....							

4. За значеннями даних матриці, $U = \|u_{kj}\|$, $k \in \overline{1,q}$, $j \in \overline{1,m}$, для стратегій, що реалізуються, визначаються оцінки за максимінним критерієм, які забезпечують гарантовано найбільшу перевагу (обсяг реалізації послуг або продукції) в найгірших умовах: $W = \max\limits_{k\in 1,q} \min\limits_{j\in 1,m} u_{kj}$.

5. Формується таблиця ризиків, у тому числі з питань ІБ, на перетині рядків і стовпців якої розміщуються значення величини ризику при реалізації даної стратегії при конкретному стані ринкової кон'юнктури, які розраховуються за формулою:

$$R_{kj} = \max_{k\in 1,q} u_{kj} - u_{kj},\ k \in \overline{1,q},\ j \in \overline{1,m},$$

де $\max\limits_{k\in 1,q} u_{kj}$ – максимально можливий обсяг продажів при фіксованому *j-ому* стану ринку X_j;

u_{kj} – обсяг продажів при реалізації фіксованої k-*ої* стратегії C_k ($k \in \overline{1,q}$) і фіксованому стані ринкової кон'юнктури та ІБ X_j ($j \in \overline{1,m}$).

6. Значення даних матриці *U*, сформованій в п.3, використовуються для обчислення мінімаксних оцінок стратегій (за Севіджем), що визначають гарантоване найменше значення ризику в якнайгіршій ситуації:

$$S = \max_{k\in 1,q} \min_{j\in 1,m} R_{kj}.$$

7. Для знаходження компромісного положення між песимістичною оцінкою за критерієм Вальда (*W*) та оптимістичною мінімаксною оцінкою (*S*), визначається значення по критерію Гурвіца (*G*) за формулою:

$$G = \max_{k\in 1,q}\left(\beta \times \min_{j\in 1,m} u_{kj} + (1-\beta) \times \max_{j\in 1,m} u_{kj}\right),$$

де β – фіксований показник песимізму-оптимізму, який визначається експертним шляхом на основі аналізу конкурентних переваг господарюючого суб'єкта і такий, що $\beta \in [0;1]$.

8. Після оцінки різних варіантів декількома критеріями, приймається рішення: якщо рекомендації співпадають, найкраще рішення обирається з більшою впевненістю; якщо спостерігається протиріччя рекомендацій, то остаточне рішення приймається з урахуванням його переваг і недоліків; наприклад, вибирається та стратегія забезпечення ІБ, яка виявилася оптимальною хоча б для двох критеріїв; якщо отримані різні стратегії для всіх трьох критеріїв, треба варіювати значеннями показника песимізму-оптимізму в критерії Гурвіца або змінити дані, наприклад, в можливих станах ринкової кон'юнктури. З урахуванням вищевикладеного, авторами пропонується наступний формалізований алгоритм побудови економетричної моделі з метою вибору оптимальної стратегії управління інвестиційним проектуванням для господарюючого суб'єкта.

Крок 0. Формування початкових даних. Формується матриця параметрів $X = \|x_j\|$ $j \in \overline{1,m}$, де m – кількість параметрів (витрат);

формується безліч припустимих стратегій $C = \{C_k\}$, $k \in \overline{1,q}$, де q – кількість стратегій

Крок 1. Вироджений крок алгоритму. За наслідками множинної регресії обчислюються прогнозні значення об'єму реалізації продукції на наступний період часу і формується

матриця $U = \left\| u_{kj} \right\|, u_{kj} = A + a_{kj} \times x_{kj}$.

Крок 2. Загальний крок алгоритму. Параметр *k:=1*.

2.1. Для k-*oї* стратегії C_k визначається значення критерію Вальда: $W_k = \min\limits_j u_{kj}$, $k \in \overline{1,q}$; значення критерію Севіджа: $S_k = \max\limits_{k \in \overline{1,q}} u_{kj} - u_{kj}$;

значення критерію Гурвіца: $G = \max\limits_{k \in \overline{1,q}} \left(\beta \times \min\limits_{j \in \overline{1,m}} u_{kj} + (1 - \beta) \times \max\limits_{j \in \overline{1,m}} u_{kj} \right)$,

де фіксоване значення $\beta \in [0;1]$.

2.2. Для кожної *k- oї* стратегії C_k, аналогічно кроку 2.1, обчислюються значення критеріїв Вальда, Севіджа і Гурвіца і формується вектор значень результатів (*Wk*, *Sk*, *Gk*).

Крок 3. Для *k < q, k:=k+1* – перехід на 3.1.

Крок 3.1. Якщо $k \geq q$, то перехід до кроку N.

Крок N. Фінальний крок алгоритму. Обчислюються:

для критерію Вальда значення $S_{k_W} = \max\limits_{k \in \overline{1,q}} W_k$;

для критерію Севіджа значення $S_{k_S} = \min\limits_{k \in \overline{1,q}} \max\limits_{j \in \overline{1,m}} S_k$;

для критерію Гурвіца значення $S_{k_G} = \max\limits_{k \in \overline{1,q}} G_k$, де S_{k_W} - індекс стратегії по Вальду, ($k \in \overline{1,q}$);

S_{k_S} – індекс стратегії по Севіджу ($k_S \in \overline{1,q}$);

S_{k_G} - індекс стратегії по Гурвіцу ($k_G \in \overline{1,q}$).

Формується оптимальна стратегія із системи умов:

якщо $S_{k_W} = S_{k_S} = S_{k_G}$, то $S_{k_e} = S_{k_W}$;

якщо $\left(S_{k_W} = S_{k_G}\right) \vee \left(S_{k_W} = S_{k_S}\right) \vee \left(S_{k_S} \neq S_{k_G}\right)$, то $S_{k_e} = S_{k_W}$;

якщо $\left(S_{k_W} = S_{k_G}\right) \vee \left(S_{k_W} \neq S_{k_S}\right) \vee \left(S_{k_S} = S_{k_G}\right)$, то $S_{k_e} = S_{k_G}$;

якщо $\left(S_{k_W} \neq S_{k_G}\right) \vee \left(S_{k_W} = S_{k_S}\right) \vee \left(S_{k_S} = S_{k_G}\right)$, то $S_{k_e} = S_{k_S}$;

якщо $S_{k_W} \neq S_{k_S} \neq S_{k_G}$, то перехід на крок 0 та зміна початкових даних.

Даний алгоритм був реалізований в програмі «Аналізатор уразливостей» [8], див. рис. 1 - 2, яка, зокрема, призначена для:

- збору інформації про стан комп'ютерів в мережі підприємства;
- оцінки поточних ризиків НСД до ІС підприємству;
- моделювання процесу ухвалення рішення по вибору оптимальної стратегії управління інвестиційним проектуванням СЗІ для господарюючого суб'єкта.

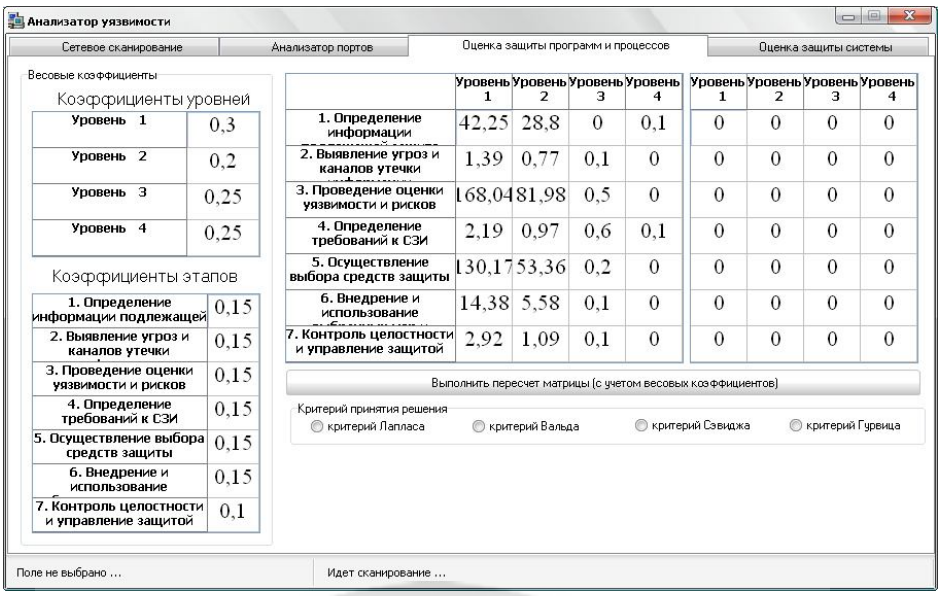

Рис. 1. Модуль програми «Аналізатор уразливостей» для моделювання процесу прийняття рішення по вибору оптимальної стратегії управління інвестиційним проектуванням СЗІ для господарюючого суб'єкта

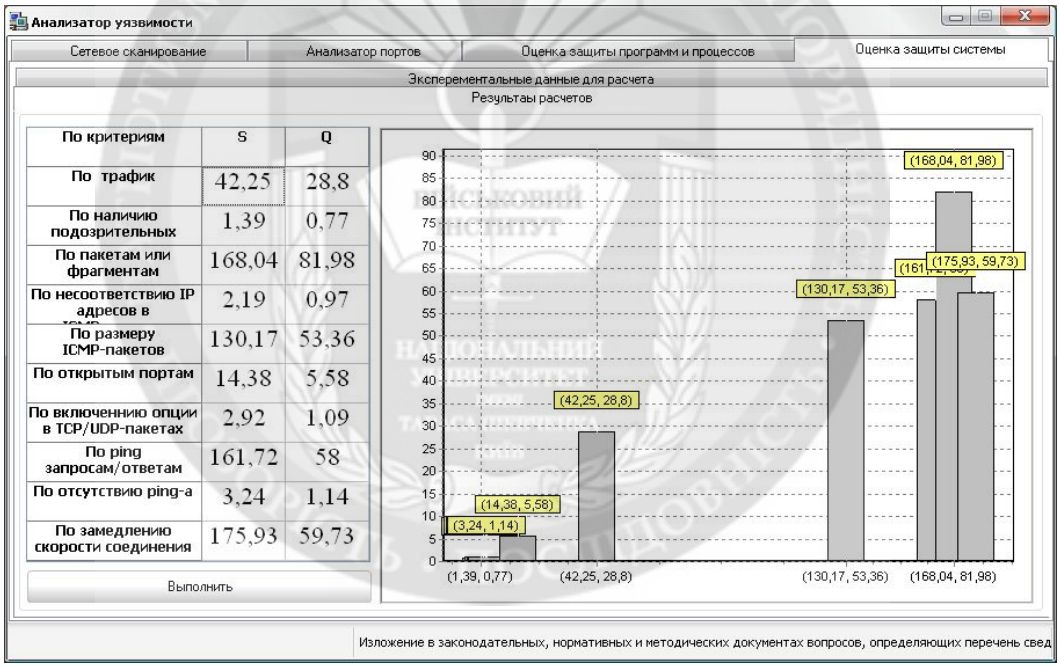

Рис. 2. Модуль програми «Аналізатор уразливостей» для оцінки ІБ господарюючого суб'єкта

Висновки. Запропонований у статті алгоритм, представляє собою детальну послідовність етапів моделювання процесу прийняття рішення щодо вибору оптимальної стратегії управління інвестиційним проектуванням СЗІ для господарюючого суб'єкта, наприклад на транспорті.

ЛІТЕРАТУРА:

1. Автоматизированные системы обработки информации и управления на автомобильном транспорте / [А.Б. Николаев, С.В. Алексахин, И.А. Кузнецов, В.Ю. Строганов]; под ред. А.Б.

Николаева. – М.: Издательский центр «Академия», 2003. – 224 с.

2. Волынская А.В. Повышение стойкости информационных систем при организации производства на транспорте: автореф. дис. на соис. уч. степ. канд. техн. наук: 05.22.01 «Транспортные и транспортно-технологические системы страны, ее регионов и городов, организация производства на транспорте» / А.В. Волынская. – Екатеринбург, 2004, 20 с.

3. Лахно В.А. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий в условиях роста транзитных перевозок. / В.А. Лахно, А.С. Петров // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – №21. – К.: ВІКНУ, 2009. – С. 110-120.

4. Тенденції розвитку загроз у 2010 році. [електронний ресурс] Режим доступу: http://eset.ua/ua/news/view/51/Tendentsii_razvitiya_ ugroz_v_2010_godu

5. Обнаружен вирус, собирающий засекреченные данные ряда стран. [электронный ресурс] Режим доступу: http://www.rbc.ua/rus/top/show/ obnaruzhen-virus-sobirayushchiy-zasekrechennye-dannye-ryada-28052012221600

6. Вирус Stuxnet атаковал ядерные объекты Ирана по приказу Обамы [электронный ресурс] / – Режим доступу: http://news.zn.ua/TECH-NOLOGIES/virus_ stuxnet_atakoval_ yadernye_obekty_irana_ po_prikazu_obamy-103090.html

7. "Лаборатория Касперского" нашла "самый сложный" вирус. [электронный ресурс] Режим доступу: http://lenta.ru/news/2012/05/28/flame/

8. Укрзалізниця повністю перейде на цифру. [електронний ресурс] Режим доступу: http://news.infocar.ua/ukrzaliznycya_ polnostyu _pereydet_ na_ cifru_ 69222.html

9. Лахно В.А. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок. Монография / В.А. Лахно, А.С Петров. - Луганск: изд-во ВНУ им. В.Даля, 2010. – 280 с.

Рецензент: д.т.н., проф. Лєнков С.В.