УДК 681.5+004
Нестеренко О.В., к.т.н., доцент
Національна академія управління
вул. Вінницька, 10, 03151, Київ, Україна
a_nest@i.ua

БЕЗПЕКОВА СИНГУЛЯРНІСТЬ

Розглянуто особливості розвитку суспільства в сучасний інформаційний період та на перспективу. Проведено аналіз загроз, що мають тенденцію до зростання у процесі подальшої технологізації різних сфер діяльності. Запропоновано можливі шляхи виходу з майбутньої кризової ситуації на основі суттєвого збільшення уваги держави до формування інтелектуального капіталу країни та підтримки індустрії програмних засобів.

Ключові слова: інформаційне суспільство, технологічна сингулярність, інформаційні технології, програмне забезпечення, кібербезпека, інтелектуальний капітал, державне управління.

Рассмотрены особенности развития общества в современный информационный период и на перспективу. Проведен анализ угроз, которые имеют тенденцию к росту в процессе дальнейшей технологізації разных сфер деятельности. Предложены возможные пути выхода из будущей кризисной ситуации на основе существенного увеличения внимания государства к формированию интеллектуального капитала страны и поддержки индустрии программных средств.

Ключевые слова: информационное общество, технологическая сингулярность, информационные технологии, программное обеспечение, кибербезопасность, интеллектуальный капитал, государственное управление.

Features development society are considered in a modern information period and on a prospect. The analysis of threats that have a tendency to height in the process of further technological different spheres of activity is conducted. The possible ways of exit from future crisis situation on the basis of substantial increase attention of the state to forming intellectual capital of country and support of software industry.

Keywords: information society, technological singularity, information technologies, software, cyber security, intellectual capital, state administration.

Вже стало реальністю, що сучасний стан проникнення інформаційно-комунікаційних технологій (ІКТ) у різні суспільні інституції, формування та розвиток національних інформаційних просторів, а через них й інформаційного середовища цивілізації, приводять до взаємозалежності технологій і сфер діяльності, та, разом із тим, до потенційної уразливості осіб, суспільства, держав, систем і обладнання, до техногенних небезпек і терористичних загроз.

Ще 2004 року колишній глава ЦРУ Джордж Тенет назвав Інтернет «ахіллесовою п’ятою США» і «чорним ходом» для терористів і ворогів. З тих часів ситуація на краще не

змінилася. Не буде перебільшенням зазначити, що вже прийшов той час, коли описані фантастами «кібервійни» стають дійсністю. Так, наприклад, стосовно зловредних програм експерти з безпеки «Лаборатории Касперского» зазначають, що «війна людей проти людей вже практично закінчена, зараз б'ються роботи проти роботів». Цей висновок витікає з того, що на цей час переважна більшість реальних загроз пов'язані з троянськими програмами, при цьому спостерігається еволюція шкідливих технологій, коли багато програм стають здатними до самореплікації. У найближчі роки очікується поява шкідливого ПЗ з людиноподібною поведінкою, здатного до адаптації і навчання на основі успішних дій. Це зробить загрози усе більш витонченими і автономними, а атаки ефективнішими і шкідливішими.

Іншим прикладом такої ефективної кіберзброї є комп'ютерні мережі, що складаються з множини хостів із активованими «ботами» (автономними програмами, установленими за допомогою троянів), так званими зомбі-машинами. Чим далі, тим ширше будуть поширюватися такі системи, що саморепліцируються. До цього слід додати, що нестримно розвивається, як в технологічному плані, так і в структурному, індустрія шкідливого програмного забезпечення (ПЗ) для мобільних пристроїв. Водночас можна стверджувати, що сучасний кіберзлочинець вже не пірат-одинак, а, швидше, ланка в серйозному бізнес-процесі з кримінальними ознаками.

Згідно з прогнозами компанії Fortinet, вже до кінця десятиліття, завдяки розвитку загроз у сфері інформаційної безпеки станеться корінний перелом. Поява нових загроз вимагає своєчасного підвищення ефективності систем безпеки на багатьох рівнях; інакше для світової віртуальної економіки настануть не найкращі часи (http://channel4it.com/).

У зв'язку із цим виникає низка запитань, пов'язаних з нашим майбутнім. До чого призведе стрімкий розвиток технологій та супутній розвиток їх небезпечних проявів? Чи можна вже сьогодні віднести явища, пов'язані з комп'ютерами і зокрема з ПЗ, до загроз безпеці цивілізації? Чому взагалі питання інформаційної та кібербезпеки так гостро стоїть на порядку денному?

Загрози інформаційній безпеці як чинники, що створюють небезпеку функціонуванню та розвитку інформаційного простору, перешкоджання інформаційним інтересам особистості, суспільства, держави, на відміну від класичних силових загроз, значення яких зменшується, відносяться до асиметричних (нетипових) [1]. Ці нові, нетрадиційні загрози є серйозною проблемою національної безпеки. Вони можуть торкатися безпеки як об'єктів і служб, істотних для злагодженого функціонування систем забезпечення життєдіяльності (критичних інфраструктур), так і безпеки окремих громадян, спільнот і держав.

Значною мірою це пов'язане із програмним забезпеченням систем управління та підтримки прийняття рішень. Інтелектуалізація систем, що набуває поширення, не лише підвищує їх ефективність, але й викликає подальше ускладнення ПЗ, утруднює його тестування та верифікацію, як наслідок – збільшує імовірність похибок та навмисного спотворення, впровадження так званих «закладок». Масовість застосування пристроїв з програмним забезпеченням, критичність таких застосувань, майбутні «Інтернет речей» та «Усеосяжний Інтернет», сучасність хмарних рішень висувають суттєві вимоги до їх надійності і безпеки функціонування. При цьому формалізується і фіксується широкий

спектр необхідних конкретних показників якості та надійності ПЗ, що використовуються. Якість стала основою конкурентоспроможності і можливості широкого застосування програмних засобів.

Фахівці швейцарської компанії Digitcapital (digitcapital.com) визначили ключові технології «завтрашнього дня», які вплинуть на IT-індустрію у найближчі кілька років. Прогнози сформовані на основі інформації, отриманої в ході ключових європейських заходів: виставки CeBIT у Гановері, стартап-конференції START Global Summit у м. Санкт-Галлен та конференції Swiss Failcon у Цюріху (рис. 1). Ці напрями головним чином пов'язані з розробкою програмного забезпечення і вони, безумовно, зроблять найбільш відчутний вплив на індустрію в наступні роки. З іншого боку, ці прогнози можуть принести й усе більш відчутні загрози для суспільства.

Рис. 1. Шість основних напрямів розвитку IT та програмного забезпечення

Важливою сферою підвищеної інформаційної небезпеки є органи державного управління, до інформаційного середовища яких кіберзлочинці проявляють зростаючу зацікавленість. Наразі вже існує чимало прикладів реалізації загроз, коли закордонні спецслужби, а також терористичні, екстремістські угруповання чи організовані злочинні групи вдаються до спроб отримання недозволеного доступу до інформації, яка не підлягає розголошенню та циркулює в системі державних органів. В умовах функціонування «електронного уряду» соціально-економічний збиток суспільства від порушень інформаційної безпеки може мати вираз у нанесенні істотних матеріальних і моральних збитків громадянам, втрати або некоректного використання персональної інформації, що може вплинути негативним чином на їхнє відношення до уряду і державної влади в цілому [2].

Фактично, мова повинна йти про таке нове питання, як «ризики процесу інформатизації». Воно пов'язане з проблемою протистояння між функціональністю інформаційних систем і їхньою безпекою, тобто суперпозицією «субоптимальності» (коли не можна оптимізувати окремі елементи системи, не погіршуючи при цьому характеристики системи в цілому) і безпеки. Реально існує якийсь компроміс, знайти який

з кожним роком стає все важче, тому що інформаційні системи ускладнюються, а вимоги щодо безпеки постійно підвищуються [3].

Інтелектуалізація систем знаходить своє найбільш яскраве відображення у створенні роботів, передусім промислового призначення. Експерти завіряють, що до 2030-2035 років 45% працюючих американців замінять комп'ютери і роботи. А за даними Morgan Stanley, в Китаї більшість робітників на заводах і фабриках замістять "розумними" механізмами вже до 2020-го року. Вже сьогодні йдеться про створення гуманоїдів/андроїдів, що будуть обслуговувати людину у побуті й на роботі, які надаватимуть безупинно відповідні послуги. Технологічна основа для створення таких істот вже формується в наші часи. Достатньо привести приклад людиноподібного робота ASIMO за проектом Honda Motor Company, здатного швидко рухатися, бігати та танцювати, реагувати на дії людей, ґрунтуючись на оцінці поточної ситуації в довкіллі, впізнавати людей одночасно по обличчю і голосу, а також розпізнавати голоси декількох осіб, що говорять навперебій. Нарешті, необхідно звернути увагу і на створення так званих кіборгів, коли застарілі частини людських організмів замінюють просто на механічний/електронний орган, що часто має більшу потужність, ніж природний.

Отже, чимало вчених і експертів наводять думки про настання кризових явищ, пов'язаних з інтенсифікацією впровадження нових технологій та розвитком робіт зі створення «штучного інтелекту». Останніми роками багатьма експертами досить живо обговорюється тема настання в найближчому майбутньому людства (орієнтовно до 2030 р.) якогось особливого моменту, так званої «точки сингулярності» - Вернор Віндж (Vernor Vinge), Рей Курцвейл (Ray Kurzweil), Константин Балашов, Андрей Новосёлов, Александр Болонкин та ін.

Прогнози подібної події так чи інакше пов'язані з аналізом феномену прискорення технологічної еволюції. Логіка цих прогнозів полягає у тому, що якщо розглянути які-небудь однотипні події в історії планети – наприклад, моменти появи істотних технічних винаходів або настання глобальних криз (не лише цивілізаційних, але і біологічних) – легко помітити, що проміжки часу між ними незмінно скорочуються. І це прискорення повинне мати якусь межу – цю саму точку сингулярності (див., наприклад, [4,5]).

Про феномен сингулярності активно і серйозно заговорили після відомої статті математика і письменника Вернора Вінджа «Технологічна сингулярность» (The Coming Technological Singularity). Цю статтю ще можна було б назвати «Чим загрожує нам штучний надрозум», оскільки в ній сингулярність як особливий момент в історії пов'язується виключно з появою штучного інтелекту як з чим-то надлюдським. Основна думка статті є такою, що за межею технологічної сингулярності людство чекає щось нелюдське, постсингулярне, і залишається лише гадати, чи зможемо ми запобігти цьому (рис. 2).

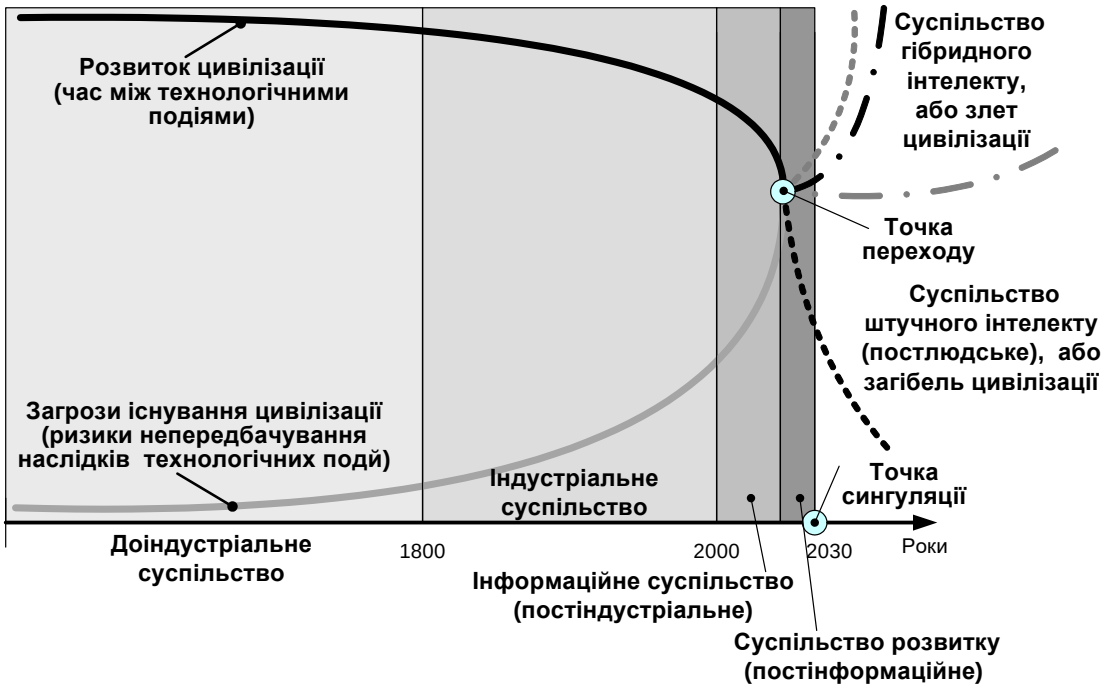

Рис. 2. Технологічна сингулярність

Окрім ризику того, що машини почнуть приймати рішення без відома людини, існує й інша небезпека – формування «провалля Мура». У якийсь момент можливості інтелектуальних систем настільки перевершуватимуть наші, що ми перестанемо розуміти механізми і логіку, що стоять за рішеннями, що приймаються ними. Лише окремі представники людства, найбільш обізнані, зможуть користуватись новими технологіями. Основна маса людей поступово припинять думати, адже інтелектуальні технології замінять людині копітку розумову працю. Залежність від кіберістот, в яку ризикує попасти людство, напевно, позначиться на подальших поколіннях, і це буде остаточною фазою існування людської цивілізації.

Чи варто боятися засилля кремнієвих "братів за розумом"? Дійсно, до кінця можливості штучного інтелекту та наслідки його реалізації поки ще не досліджені. Вочевидь, будь-який штучний інтелект має бути під контролем людського розуму. Ось тільки питання у тому, з якою метою людина буде втілювати цей контроль. Сумніватися, що знайдеться творець штучних істот, який вирішить стати володарем світу, поки не приходиться.

Тому проблеми, пов’язані із штучним інтелектом, хвилюють багатьох вчених. Один із керівників Інституту сингулярності штучного інтелекту (Singularity Institute for Artificial Intelligence - SIAI), відомого також як дослідницький інститут інтелектуальних машин (Machine Intelligence Research Institute - MIRI) (Берклі, Каліфорнія) Е. Юдковські (Eliezer Yudkowsky) у своїй роботі «Штучний інтелект як позитивний і негативний чинник глобального ризику» стверджує, що помилкова віра в те, що ШІ буде дружнім, означає очевидний шлях до глобальної катастрофи (https://intelligence.org/). При Кембриджському університеті сформований Центр вивчення існуючих загроз (Centre for the Study of Existential Risk, CSER, http://cser.org), що досліджуватиме глобальні ризики, які

потенційно приховують у собі біотехнології, нанотехнології, ядерні дослідження, антропогенна зміна клімату і розробки в області штучного інтелекту. Нарешті, більш радикально налаштовані дослідники (А. Міщенко, В. Шустров, О. Болонкин та ін.) проповідують перехід від антропоцентризму до нооцентризму та теорію Вищого Розуму – «мислячої матерії», що прийде на заміну життя на планеті, яке буде знищене розвитком техносфери (див., наприклад, http://www.ihst.ru/~biosphere/Mag_3/bolonkin.htm).

З іншого боку, багато вчених, спираючись на те, що незважаючи на неминучі кризи епох розвитку людини, кожна епоха дарувала людству нові досягнення, видатних особистостей та нову якість життя, схиляються до думки трансгуманізму, до того, що, ймовірно, наслідком епохи технологічної еволюції буде формування надінтелектуальної людини, надлюдини, досконалою як фізично, так і розумово. Найімовірніше, має бути реалізованою чергова фаза розвитку суспільства – суспільства розвитку (постінформаційного суспільства), основою якого мають стати людино-машинні системи у вигляді гібридного інтелекту [7]. Основна суть цього підходу — в об'єднанні сильних сторін людини і комп'ютера.

Чи є у сучасної людини, в окремих країн шанс підготуватись до входу у сингулярність, і навіть подолати її? Адже перспектива стати надлюдиною або технологічно-розвинутою країною світить далеко не всім. Як це було й в попередні епохи, більшість людей у власному розвитку значно відстає від тих, хто є кращими представниками суспільства. У зв'язку із цим ідеї новаторства, інновацій, особливо «освіти через усе життя», перетворення цифрової грамотності у найважливіший особистий і професійний актив, які представлені у [6,7], набувають неабиякої актуальності. Кожному потрібно дуже пильно стежити за інноваціями, щоб не пропустити момент дозрівання технологічного ривка. Для цього потрібно розвивати в себе креативність, новаторство, підтримувати творчий процес. Звісно, у цьому не обійтися без допомоги інформаційних технологій. Але важливішим є державна підтримка цього процесу, підвищена увага уряду до формування інтелектуального капіталу нації та до втілення передумов зустрічі з новою епохою. Адже тільки людина, озброєна не лише сучасними засобами інформатизації, а й відповідним знанням спроможна бути увійти в нову епоху і знайти своє місце у новому високотехнологічному світі.

Які ще потрібно зробити кроки назустріч технологічній, а точніше було б сказати - безпековій сингулярності, щоб подолати її? Необхідно зазначити, що в історичному процесі техніко-економічного переходу від промислових способів суспільного виробництва до цифрового суспільства створюється дуже складне глобальне середовище, динамічною складовою якого виступають інформаційно-комунікаційні технології і зокрема програмне забезпечення у різних своїх проявах. Завдяки стрімкому розвитку ІКТ вплив ПЗ поширюється на всі сфери суспільства. Фахівці з різних сфер вважають, що зараз програмне забезпечення здатне до управління суспільством, і як за обсягом, так і за засобами впливу воно перевищує всі інші різновиди впливу в усіх соціальних утвореннях.

Тому на сучасному етапі розвитку філософія програмного забезпечення зводиться до парадигми відкритості та свободи, відмови від уособлення влади над процесами створення найбільш поширених програм і умовами їх розповсюдження у світі [9]. Кардинальні зміни у розвитку інформаційно-аналітичного забезпечення управлінської діяльності з використанням нових інформаційних технологій, взаємовідносини влади та

суспільства, що відбуваються на цій основі, набувають вирішального значення й приводять до необхідності формування нових підходів до створення та використання ПЗ.

Разом із тим, розглядаючи реальні механізми інформатизації суспільства, необхідно звернути увагу, що цільова функція застосування ПЗ у більшості випадків або вкрай неефективна, або цілком ігнорується. Придбання та розробка ПЗ здійснюється спонтанно, без використання наукових розробок, теорії і практики побудови сучасних автоматизованих інформаційних систем. Усе це, зокрема, не дозволяє створити умови для забезпечення необхідного рівня інформаційної та кібербезпеки держави.

У кожній сфері діяльності потрібна спеціальна організація робіт із забезпечення кібербезпеки, використання специфічних форм і методів. Але існує один чинник, що є загальним для всіх сфер, і в не меншому ступені впливає на рівень безпеки — це ефективність і надійність програмного забезпечення автоматизованих систем, зокрема в критичних сферах та для підтримки прийняття рішень.

Враховуючи швидкість поширення ІКТ, їх вплив на лише на діяльність бізнесових і державних структур, а й на кожного громадянина, стрімке наближення нової епохи інтелектуалізації технічних пристроїв і пов’язаних із цим соціальних загроз вважається за необхідне вироблення відповідної державної політики, яка б надала можливість ефективного пристосування до швидкоплинних технологічних змін. Важливою складовою такої політики має стати максимальна увага держави до формування та розбудови вітчизняної індустрії програмної продукції [10, 11], створення методологічної бази вибору ПЗ та його імплементації [12]. Як приклад організації індустрії ПЗ можна навести досягнення у цій сфери Індії та Ізраїлю, що стали вже хрестоматійними, де розробка ПЗ завжди була сильною стороною хай-тек індустрії та яким притаманні основні світові тенденції розвитку ринку програмної продукції.

Перераховані вище чинники вже викликали ряд принципових змін в методології програмної індустрії, пов’язані із тим, що на зміну індивідуальному програмуванню відносно невеликих закінчених прикладних програм приходить методологія колективної, індустріальної розробки особливо складних комплексів програм з професійним розподілом праці та централізованим управлінням колективами розробників, тестувальників, маркетологів, економістів тощо.

В нас же переважна кількість публікацій та досліджень щодо вдосконалення програмної індустрії присвячені лише окремим питанням створення програмної продукції, не розкриваючи загальних тенденцій, підходів і положень щодо вироблення і використання ПЗ, не кажучи вже про пов’язані із цим ризики майбутньої цифрової цивілізації. Внаслідок цього потребують вдосконалення методи інтеграції елементів програмної індустрії в єдину державну систему на основі концептуальних чи інформаційних моделей такої системи. Заслуговують на окрему увагу розробки вітчизняних вчених, таких, наприклад, як концепція фабрик програм, що уперше сформулював академік В.М. Глушков [13].

Які можна зробити висновки? Світ стрімко рухається назустріч новим викликам цивілізації і новим загрозам, наслідки яких можуть бути непередбаченими. Вочевидь, парадигма розвитку – це основний напрям, який дозволить людству не відставати від швидкоплинного часу. Процес створення інтелектуального капіталу країни разом з

економічним розвитком має бути спрямованим на продукування, збереження та широке використання технологічних знань. Виробництво та застосування програмного забезпечення як основного засобу інтелектуалізації нових технологій повинне бути відкритим і знаходитись під посиленим контролем з боку державних органів. Це та частина, на що ми можемо вплинути. Від чого залежать рештки – ми ще не знаємо.

1. Горбулін В.П. Системно-концептуальні засади стратегії національної безпеки України / В.П. Горбулін, А.Б. Качинський. – К.: ДП «НВЦ «Євро-атлантикінформ», 2007. – 592 с.

2. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи / О.В. Нестеренко. – К.: Наук. думка, 2009. – 352с.

3. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б. Качинський; Інститут проблем національної безпеки; Національна академія Служби безпеки України. – К., 2004. – 472 с.

4. http://www.boldachev.com/text/finita-la-history/1/

5. http://www.computerra.ru/think/35636/

6. Єрмошенко М.М. Ефективний вектор прискореного розвитку – мобілізація новаторського арсеналу України на базі ІТ / М.М. Єрмошенко, В.Р. Сафонов // Інформаційні технології та спеціальна безпека, 2016, №2. – С. 2-11.

7. Єрмошенко М.М. Трансформування України у країну новаторів: концепція Національної інноваційної стратегії / М.М. Єрмошенко, Г.М. Луцький, О.В. Нестеренко, В.Р. Сафонов // Актуальні проблеми економіки. – 2012. – №12. – С. 250–254.

8. Венда В.Ф. Системы гибридного интеллекта: Эволюция, психология, інформатика / В.Ф. Венда. – М.: Машиностроение, 1990. – 448 с.

9. Будько М.М. Вільне програмне забезпечення: український вибір / М.М. Будько, О.В. Нестеренко, І.Є. Нетесін. – К.: Альтерпрес, 2011. – 400 с.

10. Поліщук В.Б. Розбудова вітчизняної індустрії програмного забезпечення - потенціал для реалізації / В.Б. Поліщук // Світ. – 2006. – № 21-22.

11. Полищук В.Б. Государство поддержит программную индустрию? / В.Б. Полищук // Computerworld/Украина, №3-4, 2008. – С.26-28.

12. Поліщук В.Б. Програмні рішення: вигоди і витрати. Методологія вибору / В.Б. Поліщук // «ИТМ. Информационные технологии для менеджмента». – 2010. - № 2,3,4,5.

13. Андон П.І. Розвиток фабрик програм в інформаційному світі / П.І. Андон, К.М. Лавріщева // Вісник Національної академії наук України. - 2010. - № 10. - С. 15-41.

Literature.

1.Gorbulin V.P. System-conceptual fundamentals of the national security strategy of Ukraine / VP Gorbulin, AB Kaczynski - Kyiv: Euro-Atlantic information, 2007. - 592 p.

2.Nesterenko O.V. Security of information space of state power. Technological bases / O.V. Nesterenko - Kyiv: Scientific Opinion, 2009. - 352p.

3.Kachinsky AB Security, Threats and Risks: Scientific Concepts and Mathematical Methods / AB Kaczynski; Institute for National Security Problems; National Academy of Security Service of Ukraine. - K., 2004. - 472 pp.

4.http://www.boldachev.com/text/finita-la-history/1/

5.http://www.computerra.ru/think/35636/

6. Yermoshenko MM An effective vector of accelerated development is the mobilization of the innovative arsenal of Ukraine on the basis of IT / MM Yermoshenko, VR Safonov // Information Technologies and Special Security, 2016, №2. - p. 2-11.

7. Yermoshenko MM Transforming Ukraine into a Country of Innovators: The Concept of National Innovation Strategy / MM Yermoshenko, GM Lutsky, O.V. Nesterenko, VR Safonov // Current problems of the economy. - 2012. - No. 12. - S. 250-254.

8. Venda VF Systems of hybrid intelligence: Evolution, psychology, informatics / V.F. Wenda. - M .: Mechanical Engineering, 1990. - 448 p.

9.Budko M.M. Free software: Ukrainian choice / M.M. Budo, O.V. Nesterenko, I.E. Netezin - Kyiv: Alternate Press, 2011. - 400 s.

10.Polishchuk VB Development of the domestic software industry - the potential for realization / VB Polishchuk // World. - 2006. - No. 21-22.

11. Polischuk V.B. Will the state support the software industry? / V.B. Polishchuk // Computerworld/ Ukraine, №3-4, 2008. – C.26-28.

12.Polishchuk VB Software solutions: benefits and costs. Selection methodology / VB Polischuk // «Information technologies for management». – 2010. - № 2,3,4,5.

13.Andon P.I. Development of software factories in the information world / P.I. Andon, K.M. Lavrischeva // Bulletin of the National Academy of Sciences of Ukraine. - 2010. - No. 10. - P. 15-41.