DOI: https://doi.org/10.36910/6775-2524-0560-2021-44-16
УДК [004.02/.032/.421] + 621.391 +004.031.42+007.2
Козубцова Леся Михайлівна, к.т.н.
https://orcid.org/0000-0002-7866-8575
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, м. Київ

УДОСКОНАЛЕННЯ ОНТОЛОГІЇ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Козубцова Л.М. Удосконалення онтології кібербезпеки інформаційної системи. У статті подано рішення науково-технічної проблеми забезпечення кібербезпеки інформаційної системи шляхом удосконалення онтології кібербезпеки. В ролі онтології кібербезпеки в роботі використано адаптовану схему стандарту ISO / IEC 15408-1. Встановлено, що у зазначеній онтології відсутні ключові принципові зворотні зв'язки. Через ці зворотні зв'язки подається «зацікавленим сторонам» інформація про рівень досягнення ефективності прийнятих рішень, здійснених заходів із забезпечення кібербезпеки. Ця інформація необхідна для розуміння ступеня досягнення кінцевої мети - кібербезпеки. Практичне значення роботи полягає в можливості отриманні інформації про ефективність прийнятих рішень та здійснених «зацікавленою стороною» заходів для розуміння ступеня досягнення кінцевої мети – кібербезпеки. Наукова новизна отриманого результату полягає в тому, що для оцінки ефективності та адекватності системи кіберзахисту «зацікавленої сторони» протистояти загрозам «Агентам загроз» відсутній зворотний зв'язок і таким чином неможливо оцінити виправданість вжитих заходів щодо збереження своїх активів.
Ключові слова: кіберзахищеність, інформаційна система, кібербезпека, онтологія, зворотній зв'язок.

Козубцова Л.М. Усовершенствование онтологии кибербезопасности информационной системы. В статье представлено решение научно-технической проблемы обеспечения кибербезопасности информационной системы путем усовершенствования онтологии кибербезопасности. В роли онтологии кибербезопасности в работе используется адаптированная схема стандарта ISO / IEC 15408-1. Установлено, что в указанной онтологии отсутствуют ключевые принципиальные обратные связи. Через эти обратные связи подается «заинтересованным сторонам» информация об уровне достижения эффективности принятых решений, осуществленных мероприятий по обеспечению кибербезопасности. Эта информация необходима для понимания степени достижения конечной цели - кибербезопасности. Практическое значение работы состоит в возможности получении информации об эффективности принятых решений и осуществленных «заинтересованной стороной» мер для понимания степени достижения конечной цели - кибербезопасности. Научная новизна полученного результата заключается в том, что для оценки эффективности и адекватности системы киберзащиты «заинтересованной стороны» противостоять угрозам «Агентам угроз» отсутствует обратная связь и таким образом невозможно оценить оправданность принятых мер по сохранению своих активов.
Ключевые слова: киберзащищенность, информационная система, кибербезопасность, онтология, обратная связь.

Kozubtsova L.M. Improving the ontology of cybersecurity of the information system. The article presents a solution to the scientific and technical problem of ensuring cybersecurity of an information system by improving the cybersecurity ontology. As a cybersecurity ontology, the paper uses an adapted scheme of the ISO / IEC 15408-1 standard. it is established that there are no key fundamental feedbacks in this ontology. Through these feedbacks, information is provided to "interested parties" about the level of achievement of the effectiveness of decisions made, measures taken to ensure cybersecurity. This information is necessary for understanding the level of achievement of the final goal - safety. The practical value of the work lies in the possibility of obtaining information about the effectiveness of the taken decisions and implemented by the "interested party" steps for understanding the degree of achievement of the final goal - safety. The scientific novelty of the obtained result lies in the fact that to assess the efficiency and adequacy of the cyber security system of the "interested party" against the threats of "Agents of Threat" there is no direct link and thus it is impossible to assess the feasibility of the implemented measures to preserve their assets.
Keywords: cybersecurity, information system, cybersecurity, ontology, feedback.

Постановка завдання і зв'язок її з важливими науковими завданнями.

Розглянемо фрагмент умовної інформаційної системи аспірантури або наукової школи (ІС НШ), яку подано на рис. 1. За вихідних даних ІС НШ функціонує і має можливість обмінюватися інформацією з зовнішнім середовищем. Під «зовнішнім середовищем» будемо розуміти мережу Інтернет з її параметрами та небезпекою у вигляді кібернетичних деструктивних інформаційних впливів.

У зв'язку з службовою необхідністю, а саме публікації наукових статей у наукових журналах включених до наукометричних баз, перевіркою наукових статей, тез доповідей, дисертацій на плагіат, тощо, ІС НШ вимушено одержувати доступу до мережі Інтернет. В результаті вона стає вразливою до деструктивних інформаційних дії «Агентів загроз». В наслідок порушення кібербезпеки – порушується кіберзахищеність, надійність ІС НШ з відповідними наслідками втрати адекватності, оптимальності, оперативності, стійкості, безперервності і скритності (останній важливий саме для ІС спеціального призначення) [1; 2].

Внаслідок безперервної появи нових вразливостей (існування вразливості нульового дня 0-day), триває пошук рішення науково-технічної проблеми забезпечення кібербезпеки ІС НШ, яка функціонує в кіберпросторі на що і буде націлене наше дослідження.

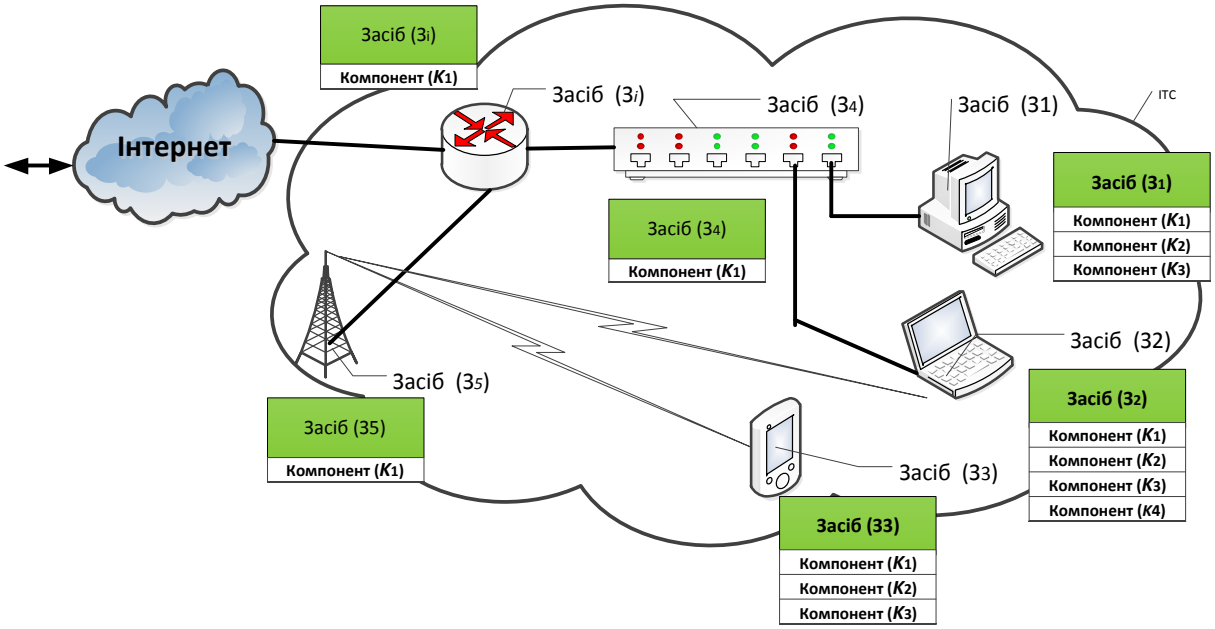

Рис.1. Фрагмент умовної ІС НШ

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій за обраним напрямком досліджень представлено в наступних публікаціях. Сформульована науково-технічна проблема не є новою, тому до нас зроблено багато спроб її вирішити. Тривалий час в наукових дослідженнях з поля зору було упущено поняття «актив» і збитків організації від втрати «активів». Саме через відсутність в зверненні понять «активи» організації, його втрати активу, що не дозволяє знаходити причинно-наслідкові зв'язки необхідної для моделювання найгіршого варіанту стану кібернетичної захищеності ІС НШ для запобігання типових загрози кібербезпеки. Авторами статті [3] розглядається підхід до визначення чисельного значення узагальненого показника цінності інформації через числові значення обраних властивостей інформації, які можливо знаходити шляхом використання апарату теорії нечітких множин, а значимість (вагу) кожної властивості – через розрахунок їх вагових коефіцієнтів методами експертного оцінювання. Авторами обрані властивості інформації – конфіденційність, цілісність та доступність, які з точки зору завдання захисту інформації впливають на саму цінність інформації та знаходяться в залежності від вибраного раціонального маршруту передачі окремих масивів інформації при умові виконання своєчасності доставки масивів інформаційного повідомлення у цілому. Отже, автори роботи оперують цінністю інформації, як активами. Це дало зорієнтувати дослідження на обґрунтуванні шляху вирішення науково-прикладної проблеми розуміння забезпечення кібербезпеки.

Мета статті. Викласти науково-прикладну проблему забезпечення кібербезпеки внаслідок відсутності зворотного зв'язку в онтології.

Виклад основного матеріалу.

Пошук рішення науково-технічної проблеми забезпечення кібербезпеки в нашому дослідженні зазначимо на алгоритм, онтологію, кібербезпеки, який подано на рис. 2. Він являє собою адаптацію відповідної схеми з ISO / IEC 15408-1 [4]. Як видно з наведеного рисунка, ключовим блоком результуючих дій є активи, при цьому метою має бути:

для «Агентів загроз» нанесення деструктивних інформаційних впливів на систему кіберзахисту для надання впливу на активи «зацікавленої сторони»;

«Зацікавлена сторона» зацікавлена докласти зусиль (виконати комплекс заходів) щодо запобігання порушенню функціонування роботи ІС від якої безпосередньо лили немає залежать збереження активів.

З відображеної на рисунку інформації не проглядається очевидний зворотний зв'язок до:

«Агентів загроз», що сигналізуватиме про ефективність виконаних заходів із застосування кіберзагроз; чи адекватні ці загрози відомим їм вразливостям ресурсів «Зацікавленої сторони». Таким чином, перевіряється ефективність та виправданість заходів;

«Зацікавленої сторони», що сигналізуватиме про ефективності системи кіберзахисту протистояти загрозам «Агентів загроз» за умови неможливості усунути всі відомі вразливості ресурсів. Таким чином виправданість зроблених заходів по збереженню своїх «Активів».

Тому штрих пунктирною лінією на рис. 2 запропоновано додати лінії зворотного зв'язку.

Необхідність у зворотному зв'язку для «Агентів загроз» обумовлена потребою розуміння, в випадку розгляду даної схеми в якості військового протиборства в кіберпросторі – «Кібернетичне протиборство», за прикладом описаного в роботах [5 – 7].

«Кібернетичне протиборство» здійснюється за допомогою кібернетичних деструктивних інформаційних впливів. Це цілеспрямоване втручання і порушення нормального функціонування за встановленим алгоритмом автоматизованих систем управління, інформаційних систем та інформаційно-телекомунікаційних мереж.

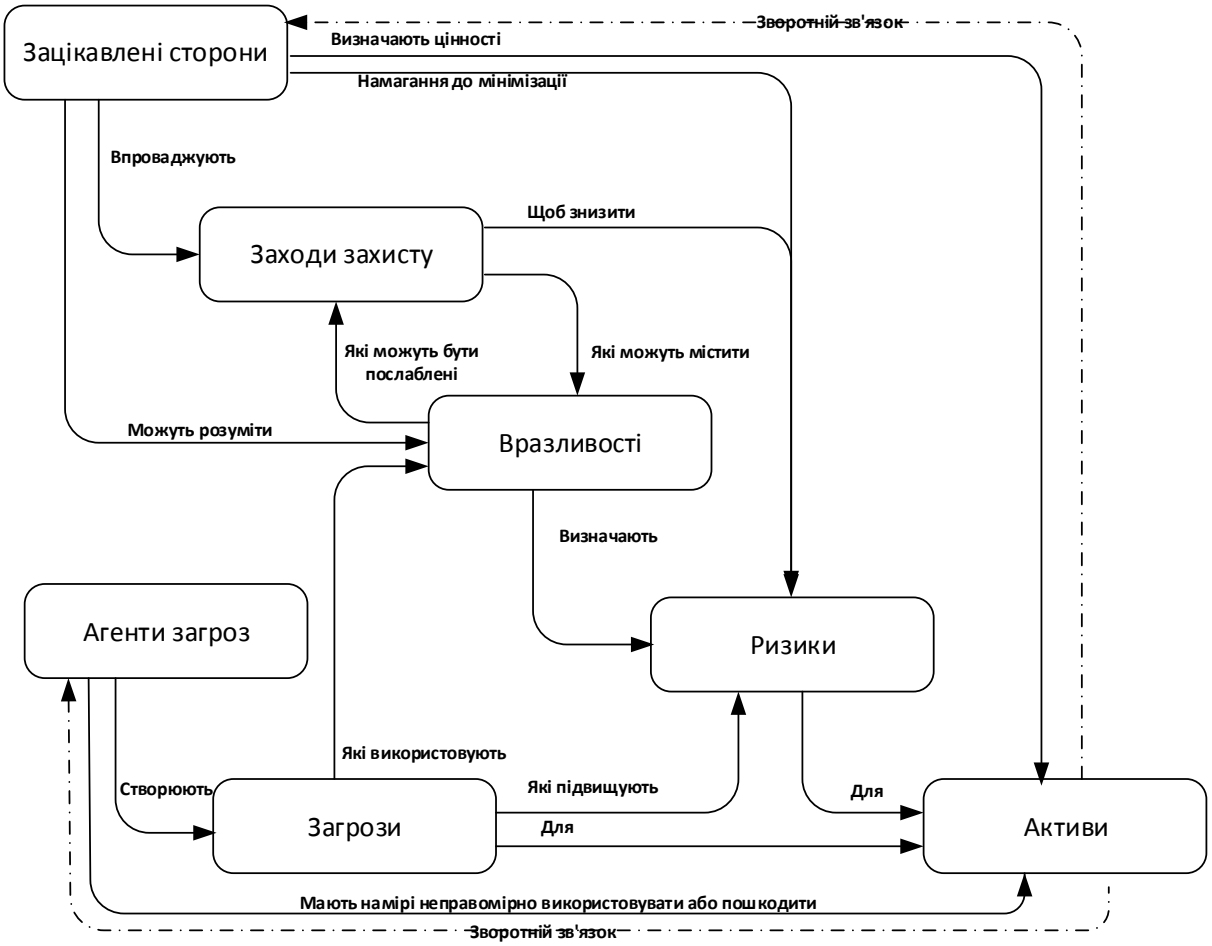

Рис.2. Функціональна залежність онтологія кібербезпеки

У разі кіберпротиборства весь процес проходить в спільному використанні загального ресурсу (глобального інформаційного простору), управління яким слід розглядати, як цілеспрямовану дію двох і більше підсистем, націлених здійснювати вплив один на одного за правилами гри з певною ймовірністю (рис. 3) [8].

Активом можуть бути людські ресурси в наслідок порушення функціонування автоматизованих систем управління військами (функціональний збій, несанкціоноване управління військами і озброєнням в результаті втрати здатності виконувати пряме призначення). Яскравим прикладом може послужити змодельовані події, що представлені в науково-фантастичному фільмі «Terminator», де штучний інтелект мережі «SkyNet» отримавши доступ до управління системою протиракетної оборони і ядерним озброєнням Збройних сил США створив умови для знищення людства. І хоча на перший погляд це виглядає фантастично, але сьогоднішні «кібервійни» і «кіберпростір», з науково-фантастичного роману В. Гібсона «Нейромант» (1982), втілилися в сучасну реальність [9].

За перерахованих наслідків можливе порушення функціонування ІС НШ, в результаті так званого інформаційно-телекомунікаційного колапсу [10].

Слід зазначити, якщо не приділити належної уваги вирішенню даного питання, то в контексті опису "Майбутнє безпекове середовище 2030. Аналіз стратегічного передбачення" додаток 2 рішення першого заступника Міністра оборони України від 26.12.2018 №401/2/4856, яке виконано дослідниками Військового інституту телекомунікацій та інформатизації за дорученням Директора Департаменту

воєнної політики, стратегічного планування та міжнародного співробітництва Міністерства оборони України в роботах [11, 12] прогнозують неминуче настання колапсу у різних сферах автоматизації та інформатизації, в тому числі:

1) небезпека спотворення, викривлення, підміна інформації у всесвітньо відомих електронних науково-технічних бібліотеках, енциклопедіях, наукометричних базах (бібліотека ім. В.І. Вернадського, Wikipedia, SciVerse Scopus, Web of Science (WoS), Google Scholar, тощо [13]);

2) втручання в роботу обладнання – атаки на комп'ютери або сервери, які забезпечують роботу цивільних комунікацій (порушення системи водопостачання, електроенергії, транспорту тощо) [14 – 16].

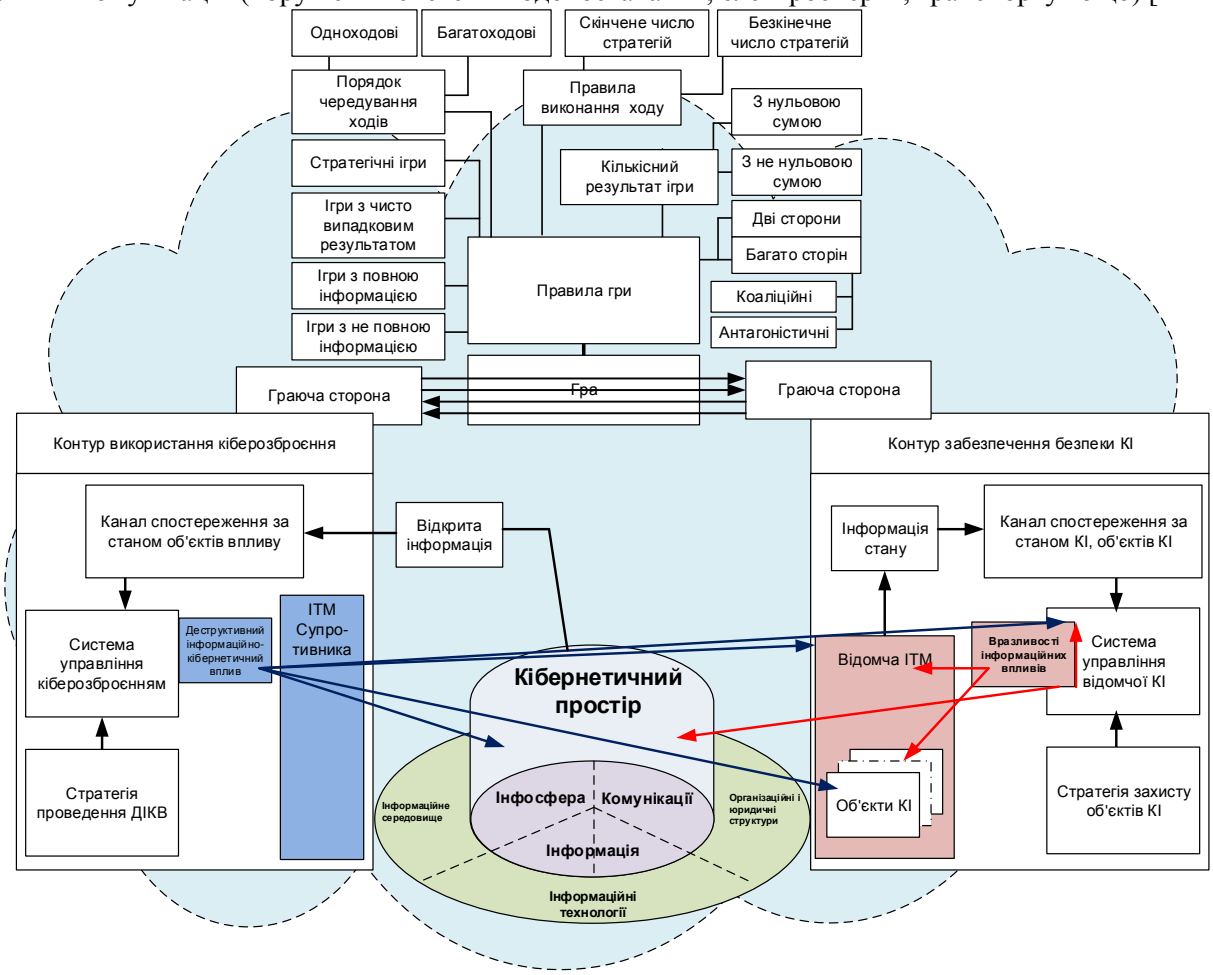

Рис.3. Модель протистояння у кіберпросторі

Висновки. Найважливішими науковим результатом дослідження, на нашу думку, стало доведення застосування зворотного зв'язку в загальній функціональні залежності реалізації кібернетичної безпеки. Оскільки через неї буде протікати інформація про процес оцінки рівня досягнення заходів з кібербезпеки заданої мети, як результат впливу «Агентів загроз» на «Активи», так і заходи захисту «Зацікавленої сторони».

Наукова новизна отриманого результату. Відсутність зворотного зв'язку від «Активів» до «Зацікавленої сторони» унеможливлює процес перевірки ефективності та виправданості реалізованих заходів. Тому можна стверджувати, що існує зворотній зв'язок від «Активів» до «Агентів загроз» оцінки ефективності реалізованих заходів кібервпливу.

Перспективи подальших досліджень доцільно застосувати удосконалену схему онтології кібербезпеки для моделювання кібербезпеки інформаційних систем.

Список бібліографічного опису

1. Боговик А.В., Игнатов В.В. Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.

2. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.

3. Куцаєв В.В., Радченко М.М., Драглюк О.В., Очіченко Р.А Оцінка узагальненого показника цінності інформації при її передачі в інформаційно-телекомунікаційній мережі. *Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]*. 2019. Вип. 4. С. 84 – 91.

4. ISO/IEC 15408-1:2005. Information technology — Security techniques — Evaluation criteria for IT security.

5. Буренок В.М., Кравченко А.Ю., Смирнов С.С. Курс на сетецентричесекую систему вооружений. *Военно-космическая оборона.* 2009. №5. URL: http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya (дата обращения 28.05.20).

6. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства. *Вопросы кибербезопасности*. 2014. № 1(2). С. 13 – 21.

7. Слипченко В.И. Войны шестого поколения оружие и военное искусство будущего. М.: Вече, 2002. 382 с.

8. Козубцов І.М., Козубцова Л.М. Стратегія гри в кібернетичному просторі. *Матеріали Міжнародної науково-технічної конференції "Сучасні інформаційно-телекомунікаційні технології"* (Київ, 17– 20 листопада 2015 р.). К.: Державний університет телекомунікацій, 2015. Том ІІІ Розвиток інформаційних технологій. С. 52 – 54.

9. Гибсон Уильям. Нейромант: Фантаст.роман / Пер. с англ. Е. Летова, М. Пчелинцева. М.: Аст; СПб.: Terra Fantastica, 2000. 317с. ISBN 5-17-000338-2.

10. Козубцов І.М., Козубцова Л.М., Терещенко Т.П., Куцаєв В.В. Глобальний колапс інформаційно-телекомунікаційних систем в наслідок порушення роботи сучасних інформаційних технологій у секторі безпеки і оборони. *Міжнародна науково-практична конференція "Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи"* (Одеса 12-13 вересня 2019 р.). Одеса. Військова академія, 2019. С. 229 – 230.

11. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П. Кібернетичні атаки як механізм створення штучного глобального колапсу інформаційно-телекомунікаційних систем. *Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф*. (Київ, 4 квітня 2019 р.). К.: Нац. акад. СБУ, 2019. С.221 – 223.

12. Козубцов І.М., Козубцова Л.М. Прогноз можливих наслідків настання "колапсу інформаційних систем спеціального призначення". *Актуальні проблеми управління інформаційною безпекою держави*: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 50 – 53.

13. Козубцов І.М., Куцаєв В.В. Філософія інформаційної безпеки в умовах її кібернетичного розповсюдження в сучасної динамічній наукової картині світу на прикладі надання знань молодим вченим та студентам. *Гілея: науковий вісник. Збірник наукових праць*. 2013. Випуск 73(№6). С. 291 – 293.

14. Кібербезпека як важлива складова всієї системи захисту держави. *Міністерство оборони України*. URL: http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (дата звернення 28.05.20).

15. Kaiser R. The Birth of cyberwar. *Political Geography*. 2015. №43. Pp. 11 – 20.

16. Thomas R., McBurney P. Cyber-Weapons. *The RUSI Journal*. Vol. 157. Iss. 1. 2012. Pp. 1 – 13.

References

1. Bogovik A.V., Ignatov V.V. Teoriya upravleniya v sistemakh voennogo naznacheniya. SPb.: VAS, 2008. 460 s.

2. Shubinskij I.B. Strukturnaya nadezhnost` informaczionny`kh sistem. Metody` analiza. M.: «Zhurnal Nadezhnost`», 2012. 216 s.

3. Kutsaiev V.V., Radchenko M.M., Drahliuk O.V., Ochichenko R.A Otsinka uzahalnenoho pokaznyka tsinnosti informatsii pry yii peredachi v informatsiino-telekomunikatsiinii merezhi. *Zbirnyk naukovykh prats [Viiskovoho instytutu telekomunikatsii ta informatyzatsii*]. 2019. Vyp. 4. S. 84 – 91.

4. ISO/IEC 15408-1:2005. Information technology — Security techniques — Evaluation criteria for IT security.

5. Burenok V.M., Kravchenko A.Yu., Smirnov S.S. Kurs na seteczentrichesekuyu sistemu vooruzhenij. *Voenno-kosmicheskaya oborona*. 2009. #5. URL: http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya (data obrashheniya 28.05.20).

6. Makarenko S.I., Chuklyaev I.I. Terminologicheskij bazis v oblasti informaczionnogo protivoborstva. *Voprosy` kiberbezopasnosti*. 2014. # 1(2). S. 13 – 21.

7. Slipchenko V.I. Vojny` shestogo pokoleniya oruzhie i voennoe iskusstvo budushhego. M.: Veche, 2002. 382 s.

8. Kozubtsov I.M., Kozubtsova L.M. Stratehiia hry v kibernetyčnomu prostori. *Materialy Mižnarodnoï naukovo-techničnoï konferentsiï "Sučasni informatsiino-telekomunikatsiini technolohiï"* (Kyïv, 17– 20 lystopada 2015 r.). K.: Deržavnyi universytet telekomunikatsii, 2015. Tom III Rozvytok informatsiinych technolohii. S. 52 – 54.

9. Gibson Uil`yam. Nejromant: Fantast.roman / Per. s angl. E. Letova, M. Pchelinczeva. M.: Ast; SPb.: Terra Fantastica, 2000. 317s. ISBN 5-17-000338-2.

10. Kozubtsov I.M., Kozubtsova L.M., Tereshchenko T.P., Kutsaiev V.V. Hlobalnyi kolaps informatsiino-telekomunikatsiinykh system v naslidok porushennia roboty suchasnykh informatsiinykh tekhnolohii u sektori bezpeky i oborony. *Mizhnarodna naukovo-praktychna konferentsiia "Spilni dii viiskovykh formuvan i pravookhoronnykh orhaniv derzhavy: problemy ta perspektyvy"* (Odesa 12-13 veresnia 2019 r.). Odesa. Viiskova akademiia, 2019. S. 229 – 230.

11. Kozubtsov I.M., Kutsaiev V.V., Kozubtsova L.M., Tereshchenko T.P. Kibernetychni ataky yak mekhanizm stvorennia shtuchnoho hlobalnoho kolapsu informatsiino-telekomunikatsiinykh system. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy: zb. tez nauk. dop. nauk.-prakt. konf*. (Kyiv, 4 kvitnia 2019 r.). K.: Nats. akad. SBU, 2019. S.221 – 223.

12. Kozubtsov I.M., Kozubtsova L.M. Proghnoz mozhlyvykh naslidkiv nastannya "kolapsu informatsiynykh system spetsial'nogho pryznatshennya". *Aktual'ni problemy upravlinnya informatsiynoyu bezpekoyu derz·havy*: zb. tez nauk. dop. nauk.-prakt. konf. (Kyyiv, 26 bereznya 2021 r.). Kyyiv: NA SBU, 2021. S. 50 – 53.

13. Kozubtsov I.M., Kutsaiev V.V. Filosofiia informatsiinoi bezpeky v umovakh yii kibernetychnoho rozpovsiudzhennia v suchasnoi dynamichnii naukovoi kartyni svitu na prykladi nadannia znan molodym vchenym ta studentam. *Hileia: naukovyi visnyk. Zbirnyk naukovykh prats*. 2013. Vypusk 73(#6). S. 291 – 293.

14. Kiberbezpeka yak vazhlyva skladova vsiiei systemy zakhystu derzhavy. *Ministerstvo oborony Ukrainy*. URL: http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (data zvernennia 28.05.20).

15. Kaiser R. The Birth of cyberwar. *Political Geography*. 2015. №43. Pp. 11 – 20.

16. Thomas R., McBurney P. Cyber-Weapons. *The RUSI Journal*. Vol. 157. Iss. 1. 2012. Pp. 1 – 13.