Безпека інформаційних систем і технологій

№ 1 (1) 2019 **НАУКОВИЙ ЖУРНАЛ**

Information systems and technologies security

Інформаційна та кібернетична безпека

ВІСНИК

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ
№ 1 (1), 2019

Свідоцтво про державну реєстрацію друкованого засобу масової інформації КВ № 23831-13671Р від 15.03.2019

Рекомендовано до друку Вченою радою факультету інформаційних технологій Київського національного університету ім. Тараса Шевченка (протокол № 3 від 21.10.2019)

Адреса редакційної колегії:

04116, Київ,

вулиця Богдана Гаврилишина, 24

Комп'ютерні науки та інформаційні технології

Журнал «Безпека інформаційних систем і технологій» було створено за ініціативою кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Т. Шевченка (протокол засідання кафедри №2 від 11.10.2018)

Підп. до друку 25.09.2019. Формат 60×84/8. Ум. друк. арк. 10,46.
Обл.-вид. арк.11,51.
Тираж 100 пр. Замовлення № 456 -2.

Видавець і виготівник
Київський національний університет ім. Тараса Шевченка
01033, Київ, вулиця Володимирська, 60

DOI: https://doi.org/10.17721/ISTS.2019.1.3-10
УДК 004.056

КОНЦЕПЦІЯ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖПРИКОРДОНСЛУЖБИ НА СТАДІЇ МОДЕРНІЗАЦІЇ

Стрельбіцький Михайло
orcid.org/0000-0001-8030-3228

м. Хмельницький, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, m.strelb@ukr.net

Історія статті:
Надійшла до редакції 25.06.2019
Прийнято 06.08.2019

Ключові слова:
концепція;
кібербезпека;
інформаційна система;
модернізація;
Держприкордонслужба.

Анотація: В статті проведено аналіз функцій прикордонної служби України та її інформаційних систем. Визначено, що модернізація складових інтегрованої інформаційної системи спричиняє порушення існуючої системи кіберзахисту. Проведений аналіз існуючих підходів до забезпечення захисту інформації в інформаційних системах показав достатньо глибоке опрацювання досліджень окремо за кожною інформаційною системою. Однак залишаються невивченими особливості взаємодії зазначених систем, зокрема при модернізації окремих інформаційних систем з точки зору забезпечення кіберзахисту загалом. Сам процес модернізації інформаційних систем здійснюється за окремими складовими системи або комплексно та вимагає їх узгодження в процесі спільного функціонування В статті наведено обґрунтування стратегій модернізації за групами критеріїв: рівня кібербезпеки, особливостей функціонування інформаційних систем. Зазначено, що значення ймовірності порушення властивостей інформаційного ресурсу змінюється протягом всього терміну модернізації. Тому обирати стратегію модернізації за значенням ймовірності в довільний момент часу є не коректним. Необхідно враховувати загальну тенденцію функції зміни зазначеної ймовірності. Найбільш доцільними є розподіл цієї групи критеріїв на три складових критерії рівня забезпечення кібербезпеки: нормативний – критерій, за якого поточне значення ймовірності порушення кібербезпеки не перевищуватиме заданого; середній – критерій, за якого середнє значення ймовірності порушення кібербезпеки не перевищуватиме заданого; зважений – критерій, за якого середнє зважене значення ймовірності порушення кібербезпеки не перевищуватиме заданого. В статті наведені функціональні залежності для визначення ймовірності порушення кібербезпеки для кожної із груп. В результаті дослідження з'ясовано, що пріоритетним показником ефективності процесу модернізації інформаційних систем прикордонного відомства є максимальне значення ймовірності порушення властивостей інформації у процесі модернізації.

Abstract: The article analyzes the functions of the Border Guard Service of Ukraine and its information systems. It is determined that the modernization of the components of the integrated information system causes a violation of the existing system of cyber defense. The analysis of existing approaches to ensuring the protection of information in information systems has shown a sufficiently deep study of research separately for each information system. However, unexperienced features of the interaction of these systems remain, in particular, with the modernization of certain information systems in terms of providing cyber defense in general. The process of modernization of information systems is carried out according to individual components of the system or complex and requires their coordination in the process of joint operation. The article gives the justification of modernization strategies according to the groups of criteria: the level of cyber security, the peculiarities of the functioning of information systems. It is noted that the value of the probability of violating the properties of the information resource varies over the entire period of modernization. Therefore, to choose the strategy of modernization at the value of probability at any time is not correct. It is necessary to take into account the general tendency of the function of changing this probability. The most expedient is the distribution of this group of criteria into three components

of the criteria for the level of cyber security: the normative - the criterion in which the current value of the probability of violating cybersecurity does not exceed the given; average - the criterion for which the average probability of a violation of cybersecurity does not exceed the prescribed; weighted - a criterion for which the average weighted probability of cybersecurity violation will not exceed the given. The article presents functional dependencies for determining the probability of cyber security violations for each of the groups. As a result of the study, it was determined that the priority indicator of the effectiveness of the process of modernizing the information systems of the border agency is the maximum value of the probability of violating the properties of information in the process of modernization.

1. ВСТУП

Виконання основних функцій Державної прикордонної служби України [1–4] з питань здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення, ведення інформаційно-аналітичної діяльності, координація діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України, пов'язане із зберіганням, обробкою та передаванням інформаційних повідомлень службового характеру між суб'єктами інтегрованого управління кордонами.

Розвиток інформаційних технологій спричинив створення на державному та відомчих рівнях великої кількості взаємно не пов'язаних інформаційних систем спрямованих здебільшого на накопичення даних та використання їх лише за напрямками діяльності суб'єктів національної безпеки. Практично повна відсутність стандартизації підходів до розробки та функціонування систем збору, обробки, аналізу, висвітлення, а саме головне ефективного обміну інформацією між суб'єктами забезпечення національної безпеки, а також технологічна комерціалізація цього напрямку досліджень є передумовою для уповільнення розвитку загальнодержавних систем моніторингу обстановки та підтримки прийняття управлінських рішень.

Інтегрована інформаційна система (ІІС) прикордонного відомства оперує критичним для прийняття рішення інформаційним ресурсом, що в свою чергу вимагає від її підсистеми кіберзахисту забезпечення дотримання всіх властивостей її інформаційних ресурсів.

В умовах складної та динамічної зміни обстановки виникає необхідність адаптації ІІС Держприкордонслужби України до потреб діяльності посадових осіб з виконання ними своїх функціональних обов'язків. Вищенаведена обставина потребує врахування підсистемою кіберзахисту факту модернізації складових інтегрованої інформаційної системи.

2. АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Значний внесок у розвиток інформаційних технологій створення гарантоздатних автоматизованих систем управління критичного застосування та захисту інформації внесли відомі вчені Бараннік В.В., Богуш В.М., Грицюк Ю.І., Грушо А.А., Дудикевич В.Б., Катеринчук І.С., Корнієнко Б.Я., Конахович Г.Ф., Ліпаєв В.В., Литвиненко О.Є., Мачалін І.О., Харченко В.С., Юдін О.К. та інші.

Проведений аналіз існуючих підходів до забезпечення захисту інформації в інформаційних системах показав достатньо глибоке опрацювання досліджень окремо за кожною інформаційною системою. Однак залишаються невивченими особливості взаємодії зазначених систем, зокрема при модернізації окремих інформаційних систем з точки зору забезпечення кіберзахисту загалом.

Інтегрована інформаційна система Держприкордонслужби України, як суб'єкта національної безпеки, має велику кількість підсистем які розподілені на всій території держави. Особливістю такої системи є вимога функціонування в реальному масштабі часу та оперування критичним для прийняття рішень інформаційним ресурсом, при чому, навіть незначне порушення властивостей якого може призвести до серйозних збитків національного масштабу [5].

При такому розумінні інформаційного ресурсу прикордонного відомства виникає потреба у забезпечені його кіберзахисту, зокрема дотриманні властивостей інформаційного ресурсу: цілісності, доступності, конфіденційності та спостереженості, тобто забезпечення комплексного кіберзахисту інтегрованої інформаційної системи прикордонного відомства в цілому [3].

Аналіз такого типу систем показав з одного

боку сталу тенденцію до зростання множини інформаційних дестабілізаційних факторів які впливають на кібернетичну безпеку, що спричинено:

розширенням умов застосування та функціонування інформаційних систем прикордонного відомства;

збільшенням кола користувачів системи, в тому числі суб'єктами інтегрованого управління кордонами;

зростанням кількості складових інтегрованої інформаційної системи;

потребою у взаємодії з міжвідомчими та міжнародними інформаційними ресурсами;

збільшенням обсягів інформації, необхідної для прийняття обґрунтованого управлінського рішення посадовими особами Держприкордонслужби;

збільшенням числа дестабілізаційних інформаційних впливів;

запровадженням нових інформаційних технологій.

З іншого боку, захист життєво важливих інтересів держави вимагає від таких систем:

забезпечення підвищених вимог з дотримання властивостей інформаційного ресурсу прикордонного відомства;

оперативності доступу до інформаційних ресурсів;

реалізації розширених можливостей щодо аналізу та узагальнення інформації;

скорочення часу для прийняття рішень;

контроль за виконанням розпоряджень.

Вищезазначене потребує постійної модернізації відомчих систем, що призводить до спільного функціонування на загальному полі даних старих, модернізованих та нових версій інформаційних систем, як складових суперсистеми. Це призводить до виникнення протиріччя між наявною теоретичною базою забезпечення кібербезпеки та потребою у постійній модернізації інформаційних систем у складі інтегрованої інформаційної системи.

Таким чином, на цій стадії життєвого циклу виникає проблема переходу на нову програмно-апаратну платформу без порушення життєвого циклу, при цьому для відомчих інформаційних систем одною з найважливіших задач є забезпечення кібербезпеки інформаційних систем, що і визначає актуальність дослідження.

Метою статті є розробка концепції кібербезпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації.

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Проведений аналіз підходів до забезпечення кібернетичної безпеки в інтегрованих інформаційних системах показав, що більшість досліджень зосереджені на проблемах захисту інформації окремо в кожній інформаційній системі. Уперше уніфіковану концепцію захисту інформації запропонував Герасименко В. А. [6]

Застосування зазначеної концепції створює передумови для впровадження всіх досліджень в галузі захисту інформації, а саме: структурованого середовища захисту, всебічної оцінки уразливості інформації залежно від дії дестабілізаційних факторів зовнішніх та внутрішніх загроз, формування вимог до захисту, побудова системи захисту інформації в залежності від умов функціонування, формування рекомендацій з підвищення ефективності захисту.

Концепція загалом передбачає циклічний процес вдосконалення системи захисту інформації. Разом із тим, сам процес модернізації, його методологічні засади в уніфікованій концепції не розглянуті. Для наявних систем захисту, які реалізовані в сучасних ІС, загалом не передбачається спільного функціонування різних версій програмно-апаратного забезпечення, систем захисту тощо. Вищенаведене вимагає структурованого аналізу та декомпозиції факторів, що впливають на дотримання властивостей інформації на стадії модернізації.

Сам процес модернізації інформаційних систем здійснюється за окремими складовими системи або комплексно та загалом вимагає їх узгодження в процесі спільного функціонування (рис. 1).

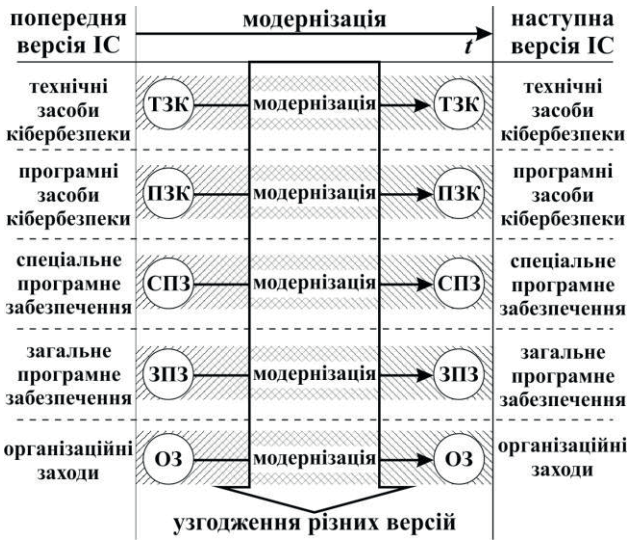


Рис. 1 – Структура процесу модернізації ІС

Отже, з точки зору кібербезпеки модернізація вимагає формулювання стратегії як головної

мети зазначеного процесу. Стратегія кібербезпеки на стадії модернізації як модель узагальнених дій, спрямованих на досягнення зазначеної мети, полягає у такій сукупності заходів по заміні складових інформаційної системи (ІС), за якої рівень кібербезпеки відповідає нормативному.

Водночас, умови функціонування різних інформаційних систем, їх структура та вимоги до кібербезпеки можуть суттєво відрізнятись. Через це загальне формулювання стратегії кібербезпеки на стадії модернізації може дещо відрізнятись один від одного. Загалом, організація процесу модернізації в рамках розглянутої стратегії полягає в пошуку раціонального співвідношення між вимогами до нової версії ІС та рівнем інформаційних дестабілізаційних факторів, викликаних невідповідністю версій. Таке формулювання проблеми належить до галузі оптимізаційних завдань. Разом із тим, значна кількість випадкових факторів не дозволяє сформувати функціональні залежності для їх вирішення відомими оптимізаційними методами.

Обґрунтування стратегій модернізації будемо здійснювати за групами критеріїв: рівня кібербезпеки та особливостей функціонування ІС.

Формуванню першої групи критеріїв присвячена велика кількість робіт [7–11], в яких дослідники обґрунтовують його фізичний сенс. У більшості досліджень як показник рівня кібербезпеки пропонується використовувати ймовірність попередження шкоди, враховуючи стохастичну природу дестабілізаційних впливів. Варто зазначити, що значення ймовірності виникнення шкоди протягом всього терміну модернізації буде різною, тобто $P(t)$. Так обирати стратегію модернізації за значенням ймовірності в довільний момент часу є не коректним. Необхідно враховувати загальну тенденцію функції зміни зазначеної ймовірності.

На наш погляд, найбільш доцільними є розподіл цієї групи критеріїв на три складових критерії рівня забезпечення кібербезпеки:

нормативний – критерій, за якого поточне значення ймовірності порушення кібербезпеки не перевищуватиме заданого;

середній – критерій, за якого середнє значення ймовірності порушення кібербезпеки не перевищуватиме заданого;

зважений – критерій, за якого середнє зважене значення ймовірності порушення функціональної безпеки не перевищуватиме заданого.

Друга група критеріїв, яка визначає особливості функціонування ІС [12–14] на стадії модернізації, характеризує можливості щодо втручання в процес роботи системи. За цією групою критерії поділяються на три види:

системи реального часу характеризуються практичною відсутністю будь-яких можливостей щодо втручання в процес їх функціонування. Прикладом такої системи є ІС "Гарт-1", система автоматизації пропуску осіб, транспортних засобів через державний кордон України. Зупинка такої системи навіть на невеликий термін є недопустимою, оскільки може призвести до збитків національного масштабу;

системи з можливістю часткової зупинки характеризуються більшими можливостями для процесу модернізації. Прикладом такої ІС може бути "Гарт-5", система автоматизації інформаційно-аналітичної діяльності. Ці системи функціонують, як правило, під час робочого дня, тобто третину доби.

системи з можливістю повної зупинки характеризуються максимальними можливостями для процесу модернізації. Такого типу системи мають обмеження тільки терміном експлуатації.

Вищенаведене дозволяє сформувати узагальнену таблицю раціональних стратегій модернізації як декартового добутку обох критеріїв (таблиця 1)

Отже, нормативний рівень варто застосовувати до систем реального часу з причини забезпечення неперевищення значення ймовірності порушення кібербезпеки протягом всього терміну модернізації.

Таблиця 1 – Раціональні стратегії модернізації

Критерій рівня забезпечення кібербезпеки	Особливості ІС		
	реального часу	часткова зупинка	повна зупинка
Нормативний	+	–	–
Середній	–	+	–
Зважений	–	+	–

Середній та зважений критерії захисту доцільно використовувати при модернізації систем з можливістю часткової зупинки функціонування. Вибір критерію залежить від величин часу та періодичності часткової зупини системи.

Такі дослідження дозволяють сформувати загальну концепцію забезпечення кібербезпеки ІС на стадії модернізації як інструментально-методологічну базу що забезпечує виконання розглянутих стратегій (рис.2).

Першочерговим етапом є обґрунтування самого об’єкту системи кібербезпеки. Саме від визначення цього поняття та його властивостей залежить формування всієї концепції кібербезпеки на стадії модернізації. Разом із тим,

ключовим питанням є визначення стратегії модернізації як напрямку зосередження основних зусиль всієї системи. Базуючись на визначених обох складових, здійснюється узгодження різних версій ІС.

У більшості випадків модернізація загального програмного забезпечення не здійснює впливу на уразливість ІС з причини завчасної перевірки можливості функціонування різних версій [15]. Загальне програмне забезпечення не є частиною ІС, а використовується як платформа для функціонування спеціального програмного забезпечення (СПЗ) на конкретному автоматизованому робочому місці (АРМ) або серверному обладнанні. Організаційні заходи, що спрямовані на забезпечення кібербезпеки, теж не є складовою ІС, хоча здійснюють вплив на процес кібербезпеки. Ці два елементи виходять за межі дослідження та не включені в загальну концепцію забезпечення кібербезпеки на стадії модернізації.

Рис. 2 – Загальна концепція забезпечення кібербезпеки на стадії модернізації

Здійснювати завдання узгодження різних версій ІС необхідно тільки в умовах їх спільного функціонування через врахування основного припущенням дослідження, що в різних версіях ІС окремо кібербезпека забезпечується відповідно до встановлених вимог. Отже, в системах з можливістю повної зупинки функціонування на період модернізації не виникають дестабілізаційні фактори, викликані спільним функціонуванням різних версій ІС.

Концепцією передбачено три завдання узгодження. Перше завдання – це узгодження спільного функціонування спеціального програмного забезпечення АРМ інформаційних систем. Модернізація СПЗ здійснюється фахівцями відділів зв'язку, автоматизації та захисту інформації почергово кожного АРМ. Так виникає ситуація спільного функціонування в системі АРМ з різними версіями СПЗ. Вирішення цього завдання можливе шляхом визначення раціональної послідовності модернізації АРМ в інформаційній системі відповідно до обраної стратегії забезпечення кібербезпеки.

Другим завданням є узгодження програмних засобів захисту, а саме розробка сукупності методів узгодження систем розмежування доступу до інформаційних ресурсів ІС та на їх основі формування методологічного базису. Вирішення цього завдання дозволить науково обґрунтувати принципову можливість функціонування різних версій систем розмежування доступу на спільному полі даних.

Третім завданням є вдосконалення технічних (апаратних) засобів забезпечення кібербезпеки. Під час модернізації ІІС можлива зміна структури технічних засобів забезпечення кібербезпеки. Це вимагає вирішення завдання раціонального їх розподілу на стадії модернізації з урахуванням взаємодії наявних та доданих засобів, а також вимог до загального рівня безпеки інформаційної системи.

Наступними етапами концепції є визначення величини уразливості даних при проведенні заходів з модернізації та оцінювання ефективності кібербезпеки в ІС на стадії модернізації. На даних етапах враховуються умови функціонування системи та вплив зовнішнього середовища на процес кібербезпеки. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення щодо проведення модернізації та визначення організаційних заходів з особливості проведення самого процесу оновлення складових ІС.

Сформуємо показники ефективності за різними стратегіями модернізації.

Перший. Повна зупинка функціонування ІС та здійснення заміни визначених програмних елементів з подальшим введенням в експлуатацію зазначеної системи. Цей спосіб з точки зору кібербезпеки є найбільш раціональним. В даному випадку взагалі виключена можливість реалізації загроз, викликаних процесом модернізації. Водночас застосування першого підходу можливе тільки на невеликих системах та й на таких, які не мають вимоги функціонування в режимі

реального часу. Як правило, вимогою до переважної більшості інформаційних систем та підсистем ІІС прикордонного відомства є цілодобове функціонування. Навіть невеликий збій може призвести до непоправних збитків національного масштабу. Територіальна розподіленість елементів окремих ІС та достатньо велика їх кількість при застосуванні першого підходу вимагатиме досить значного часу на проведення модернізації. Використання такого підходу в прикордонній службі є неприпустимим.

Другий підхід передбачає модернізацію ІС в процесі її функціонування. У цьому випадку можливе порушення властивостей інформаційного ресурсу ІС і, в свою чергу, кіберзахисту, оскільки з'являються додаткові дестабілізаційні фактори, викликані невідповідністю версій СПЗ. Отже, головним чинником, який визначатиме ефективність процесу модернізації, є максимально можливе зменшення ймовірності порушення властивостей інформаційного ресурсу. Разом із тим, варто зазначити, що модернізація ІС це процес, який має певну тривалість та не може бути описаний окремими точковими показниками поза межами часу.

Визначимо основні показники, які характеризують ефективність процесу модернізації: $P_M(t)$ – ймовірність порушення властивостей інформаційного ресурсу; t_M – загальний час модернізації.

Різні варіанти модернізації можна порівняти за загальним часом модернізації, але в більшості випадків він задається директивно та не відображає величину порушення властивостей інформаційного ресурсу. Отже, цей показник може бути тільки як допоміжний у випадку рівності інших показників. З іншого боку порівнювати різні варіанти послідовності модернізації елементів ІС за миттєвим значенням ймовірності порушення властивостей інформаційного ресурсу є неможливим з причини її зміни протягом всього терміну модернізації.

Вищенаведене вимагає використання інтегрованих показників, що характеризують весь процес модернізації. Одним із показників такого типу є максимально можливе значення ймовірності порушення властивостей інформаційного ресурсу в процесі модернізації

$$P_M^{\max} = \max_{0 \le t \le t_M} \left(P_M(t) \right). \quad (1)$$

Перевагою цього показника є можливість визначення допустимого значення ймовірності порушення інформаційного ресурсу на стадії модернізації.

Наступним показником, який характеризує ефективність процесу модернізації, є середнє значення ймовірності порушення властивостей інформаційного ресурсу в процесі модернізації.

В інтегральній формі

$$P_M^{mid} = \frac{1}{t_M} \int_0^{t_M} P_M(t) dt \quad (2)$$

У дискретній формі

$$P_M^{mid} = \frac{1}{N} \sum_{i=1}^{N} P_M(t_i) \quad (3)$$

де N – кількість інтервалів вимірювання значення ймовірності.

Такий показник доцільно застосовувати при забезпеченні якомога меншого значення ймовірності порушення властивостей інформаційного ресурсу під час модернізації. Вибір показника ефективності залежить від способу застосування ІС та процесу її модернізації.

Наступним показником ефективності процесу модернізації може бути середньозважене значення ймовірності порушення властивостей інформаційного ресурсу.

В інтегральній формі

$$P_M^w = \frac{1}{t_M} \int_0^{t_M} f^w(t) P_M(t) dt, \quad (4)$$

де $f^w(t)$ – функція ваги.

За умови, що

$$\int_0^{t_M} f^w(t) dt = 1. \quad (5)$$

У дискретній формі

$$P_M^w = \frac{1}{N} \sum_{i=1}^{N} f^w(t_i) P_M(t_i). \quad (6)$$

За умови, що

$$\sum_{i=1}^{N} f^w(t_i) = 1. \quad (7)$$

Пріоритетним показником ефективності процесу модернізації для більшості ІС прикордонного відомства є максимальне значення ймовірності порушення властивостей інформаційного ресурсу в процесі модернізації. Чим менше цей показник, тим ефективніше провадиться заміна СПЗ на елементах ІС. При рівності значень цього показника в різних

варіантах модернізації доцільно застосувати другий або третій показники.

4. ВИСНОВКИ

Аналіз існуючих підходів до проблеми забезпечення кібербезпеки показав наявність циклічного процесу вдосконалення такого типу систем. Водночас, сам процес модернізації, його методологічні засади у цих підходах не розглянуті. Для наявних систем забезпечення кібербезпеки, які реалізовані в сучасних ІС, загалом не передбачається спільного функціонування різних версій програмно-апаратного забезпечення, систем забезпечення кібербезпеки безпеки, тощо. Це вимагає структурованого аналізу та декомпозиції факторів, що впливають на дотримання властивостей інформаційної системи на стадії модернізації.

Опис процесу модернізації ІС дозволив сформулювати стратегію кібербезпеки, яка полягає у такій сукупності заходів по заміні складових інформаційної системи, за якої рівень кібербезпеки відповідав нормативному. Разом із тим, умови функціонування різних ІС, їх структура та вимоги до кібербезпеки можуть суттєво відрізнятись. Через це загальне формулювання стратегії кібербезпеки на стадії модернізації може дещо відрізнятись один від одного. Аналіз критеріїв та особливостей функціонування дозволив сформувати раціональні стратегії модернізації.

Вищенаведені дослідження дозволили сформувати загальну концепцію кібербезпеки на стадії модернізації як інструментально-методологічну базу, що забезпечує виконання розглянутих стратегій. Концепцією передбачено три завдання узгодження спільного функціонування: спеціального програмного забезпечення, програмних та технічних (апаратних) засобів забезпечення кібербезпеки, а також визначення величини уразливості інформаційного ресурсу системи при проведенні заходів з модернізації та оцінювання ефективності кібернетичної безпеки в ІС на стадії модернізації. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення щодо проведення модернізації та визначення організаційних заходів щодо особливості проведення самого процесу оновлення складових ІС.

Визначення раціональної стратегії модернізації вимагає обґрунтування показників ефективності здійснення процесу модернізації. Аналіз особливостей функціонування різних ІС дозволив сформувати три види показників: за максимально можливим значенням ймовірності порушення властивостей інформаційного ресурсу під час модернізації, за середнім значенням ймовірності порушення властивостей інформаційного ресурсу у процесі модернізації та середньозваженим значення ймовірності. З'ясовано, що пріоритетним показником ефективності процесу модернізації для більшості ІС прикордонного відомства є максимальне значення ймовірності порушення його властивостей у процесі модернізації. Чим менше цей показник, тим ефективніше провадиться заміна СПЗ на елементах інформаційної системи.

5. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Про основи національної безпеки України: Закон України // *Офіційний Вісник України*. – 2003. – № 39. – Ст. 351.

[2] *Доктрина "Інформаційної безпеки України"* [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство.

[3] Стрельбіцький М.А. "Прикордонний інформаційний ресурс: визначення поняття" *Сучасні інформаційні технології у сфері безпеки та оборони*. Національний університет оборони України імені Івана Черняховського №1 (25) 2016. С. 205-208

[4] Липаев В.В. *Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств*. / В.В. Липаев // Информационный бюллетень "JetInfo". – 2003. – № 3 (130). – 27 с.

[5] Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство.

[6] Герасименко В. А. *Защита информации в АСОД* (в 2-х томах). – М.: Энергоатомиздат, 1994. – 400 с.

[7] Харибін О. В. "Інформаційна технологія забезпечення функціональної безпеки бортових інформаційно-керуючих систем авіації на етапі експлуатації" *Системи озброєння і військова техніка* № 2. – 2010. – С. 173-177.

[8] І. В. Муляр, А. В. Джулій, М. В. Костюк "Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних" *Вимірювальна та обчислювальна техніка в технологічних процесах*. – 2013. – № 1. – С. 133-138.

[9] Манжос Ю. С. "Використання аналізу розмірностей для підвищення рівня

функціональної безпеки I&C систем" *Радіоелектронні і комп'ютерні системи* № 7. – 2012. – С. 313-318.

[10] С. Г. Семенов, С. Ю. Гавриленко, Кассем Халіфе "GERT-модель прогнозування параметрів функціональної безпеки технічних систем" *Системи обробки інформації* № 2. – 2016. – С. 50-52.

[11] Борзов Ю. *Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування*. Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук / Львівський державний університет безпеки життєдіяльності. м. Львів (2015).

[12] К. В. Юдкова, Г. Г. Чернишина "Класифікація інформаційних систем" *Інформація і право* № 3. – 2015. – С. 92-98.

[13] Гужва В. М. *Інформаційні системи і технології на підприємствах*. К.: КНЕУ (2001): 133-170.

[14] П. П. Маслянко, П. М. Ліссов "Інформаційно-комунікаційні системи та технології обробки інформаційних ресурсів" *Вісн. КУЕІТУ "Нові технології* № 1-2. – 2007. – С. 15-16.

[15] Стрельбіцький М. А. "Декомпозиція технології захисту інформації в корпоративних системах" *Збірник наукових праць Національної академії Державної прикордонної служби України*. № 59: – С. 296-301.

***Стрельбіцький Михайло Анатолійович**, **доктор технічних наук, доцент**, начальник (завідувач) кафедри зв'язку, автоматизації та кібербезпеки Національної академії Державної прикордонної служби України імені Богдана Хмельницького. Закінчив військову інженерно-космічну академію імені О.Ф. Можайського, область наукових інтересів: кібербезпека, функціональна безпека, інформаційна безпека*

DOI: https://doi.org/10.17721/ISTS.2019.1.11-18
УДК 004.056.5

РЕАЛІЗАЦІЯ ГРУПОВОГО ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ ТА РІВНЯ ГАРАНТІЙ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Бучик Сергій [1]
orcid.org/0000-0003-0892-3494
Юдін Олександр [2]
orcid.org/0000-0002-6417-0768
Нетребко Руслан [3]
orcid.org/0000-0003-3212-5249

[1] м. Київ, Київський національний університет імені Тараса Шевченко, buchyk@knu.ua
[2] м. Київ, Київський національний університет імені Тараса Шевченко, yak333@ukr.net
[3] м. Житомир, Житомирський військовий інституту імені С.П. Корольова, netr_rv@ukr.net

Історія статті:
Надійшла до редакції 28.06.2019
Прийнято 12.07.2019

Ключові слова:
інформаційно-телекомунікаційна система;
автоматизована система;
інформаційна безпека;
функціональний профіль захищеності;
рівень гарантій;
політика безпеки інформації;
правила розмежування доступу;
несанкціонований доступ;
комплекс засобів захисту;
експертна інформація.

Анотація: У статті запропоновано, показано та проаналізовано основні етапи реалізації програмного забезпечення по груповій оцінці функціонального профілю та визначення або узгодження рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації інформаційно-телекомунікаційних систем від несанкціонованого доступу в Україні на основі раніше проведених авторами теоретичних досліджень. Висвітлено необхідні нормативні документи технічного захисту інформації, які регламентують порядок оцінки та визначення рівня гарантій автоматизованих систем від несанкціонованого доступу в Україні. Здійснено проектування роботи програми за допомогою діаграм Data Flow Diagram, а саме: розроблені контекстна діаграма процесу групового визначення та декомпозована діаграма процесу групового визначення функціональних профілів захищеності та рівня гарантій. Побудовані більш детальні блок-схеми роботи програмного забезпечення та алгоритмів, які реалізовані в прототипі програмного забезпечення. Приведено приклади роботи по кожному з основних блоків роботи, які були попередньо спроектовані в діаграмах та блок-схемах алгоритмів. Визначені переваги та недоліки розробленого програмного забезпечення групового визначення функціонального профілю захищеності та рівня гарантій. Розроблена програма дозволяє провести групову оцінку та порівняти результати відправлені на сервер. Даний підхід дозволяє зменшити час, який витрачає адміністратор безпеки для визначення функціональних профілів захищеності та рівнів гарантій оброблюваної інформації від несанкціонованого доступу, та виявити наявність співпадіння визначеного функціонального профілю із стандартним (за умови виконання даного співпадіння користувачу надається інформація про даний стандартний функціональний профіль) та підтвердити або визначити інший рівень гарантій. За рахунок проведення групової експертизи підвищується достовірність отриманих результатів.

Abstract: The article proposes, shows and analyzes the main stages of implementing software for group assessment of a functional profile and determining or agreeing the level of guarantees for the correct implementation of functional security services in information security tools of information of telecommunication systems from unauthorized access in Ukraine based on theoretical studies previously conducted. The necessary regulatory documents on technical protection of information governing the procedure of evaluating and determining the level of guarantees of automated systems against unauthorized access in Ukraine are covered. The program was designed using the Data Flow Diagram, namely, a contextual diagram of the group definition process and a decomposed diagram of the process of group determination of the functional security profiles and the level of guarantees. More detailed flowcharts of software and algorithms are constructed. A prototype of the software is implemented;

examples of work on each of the main blocks of work that were previously designed in the diagrams and flowcharts of the algorithms are given.
Certain advantages and disadvantages of the developed software for group determination of the functional security profile and the level of guarantees are defined. The developed program allows to carry out group estimation and to compare the results sent to the server. This approach reduces the time spent by the security administrator to determine the security profiles and security levels of the information being processed against unauthorized access and to detect whether a specified functional profile coincides with a standard one (provided this match the user is provided with information about that standard functional profile) or determine another level of warranty. By conducting a group examination, the reliability of the obtained results increases.

1. ВСТУП

Стрімке зростання новітніх технологій, а також розвиток інфраструктури інформаційно-комунікаційних мереж державного та загального призначення призвело до створення інтегрованого інформаційного простору держави та всього суспільства. Інформаційні технології знаходять усе ширше застосування в таких сферах, як: державні системи управління, фінансовий обіг і ринок цінних паперів, розвинута система електронних платежів, система послуг зв'язку та телебачення, системи управління транспортом, високотехнологічні виробництва (особливо атомні, хімічні тощо) і т. ін. Будь-яке несанкціоноване та протиправне втручання в інформаційний простір наведених сфер життєдіяльності держави й суспільства може призвести до тяжких та не передбачуваних наслідків [1].

Досліджуючи нормативно-правову базу (НПБ) України в галузі захисту інформаційно-телекомунікаційних систем (ІТС) від несанкціонованого доступу (НСД), слід відмітити наступні документи:

- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 [2];
- НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24 липня 2009 року № 172 [3].

Саме дані документи стали основою для проведення аналізу та подальшого дослідження.

В розрізі продовження дослідження є актуальним здійснити формалізацію теоретичних основ групового визначення функціонального профілю захищеності та рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу та реалізувати програмно, що дозволить автоматизувати процес визначення та зменшить витрати часу та матеріальних (людських) ресурсів, які витрачаються на такий процес. Також, за рахунок проведення групової експертизи, підвищиться достовірність отриманих даних.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналіз останніх досліджень і публікацій показав, що питання розвитку систем захисту, їх створення, організації та дослідження процесів їх функціонування відображенні в працях багатоьох вітчизняних і закордонних вчених. Так багато праць Баранніка В.В. присвячені захисту відеоінформаційних ресурсів [4,5], Юдіна О.К. та Конаховича Г.Ф. захисту інформації в мережах передачи даних, комп'ютерній стеганографії [6,7], Новікова О.М. безпеці інформаційно-телекомунікаційних систем [8] і т.ін. Дані праці показують основні теоретичні положення з захисту інформації, методологічні та науково-теоретичні основи побудови систем захисту, оцінки їх ефективності та принципів вибору параметрів для оцінки ефективності. Також в окремих працях проаналізовано використання методів перевірки несуперечності та повноти профілю захищеності від НСД, побудови таксономії функціональних послуг безпеки від НСД, парето-оптимальних ФПЗ [9,10,11,12]. В роботі [13] проведено системний аналіз профілю захищеності відкритих інформаційних систем, розкрита відома структура критеріїв. Тематиці визначення групової оцінки функціонального профілю та рівня гарантій ІТС від НСД присвячено небагато робіт, що на думку авторів

пов'язано з тим, що процес визначення здійснюється експертною комісією та фактично єдиними документами, які визначають підходи до визначення ФПЗ та гарантій. Дана робота є продовженням роботи реалізація програмного продукту визначення функціональних профілів та рівня гарантій автоматизованих систем від несанкціонованого доступу на основі НПБ [14] та тематики робіт над якими працює група науковців. Тому наразі стоїть питання можливості групової оцінки ФПЗ та запропонованого рівня гарантій автоматизовано на основі НПБ. Раніше авторами було розроблено програмне забезпечення визначення функціональних профілів та рівня гарантій ІТС від несанкціонованого доступу (А.с. 74344 Україна. Комп'ютерна програма. Інформаційна система визначення функціонального профілю захищеності та рівня гарантій автоматизованої системи від несанкціонованого доступу (ОФПАС 2.0)), але дане програмне забезпечення було розраховане на одного експерта. Тому актуальним стоїть питання впровадження групової оцінки.

3. МЕТА СТАТТІ

Здійснити реалізацію теоретичних основ групової оцінки визначення ФПЗ та рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованої системи від несанкціонованого доступу та розробити прототип програмного забезпечення.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Швидкий розвиток інформаційних технологій потребує значного захисту інформації користувачів різних рівнів. Починаючи з двохтисячних років розроблялась НПБ України щодо захисту інформації, оцінки ступеня захисту ІТС.

З визначенням стандартних функціональних профілів захищеності та рівнів гарантій пов'язана ціла низка нормативних документів технічного захисту інформації (НД ТЗІ), а саме: НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, НД ТЗІ 2.7-010-09. Проаналізувавши дані документи було визначено, що ці документи надають лише методологічну базу з точки зору, як нормативний документ для вибору та реалізації вимог безпеки в ІТС, але єдиної методології, яка б поєднувала дані документи та надавала зрозумілу та просту інтерпретацію процесу обирання ФПЗ та рівнів гарантій немає, тому було реалізоване програмне забезпечення для роботи одного експерта. В зв'язку з чим, актуальним є створення системи для визначення групової оцінки, тобто мережевої версії.

У ході дослідження методу авторами було проведено моделювання процесів групового визначення. На рис. 1 наведено головну контекстну діаграму процесу групового визначення ФПЗ та рівня гарантій, на рис. 2 – результат моделювання підпроцесів групового визначення ФПЗ та рівня гарантій проміжного рівня деталізації.

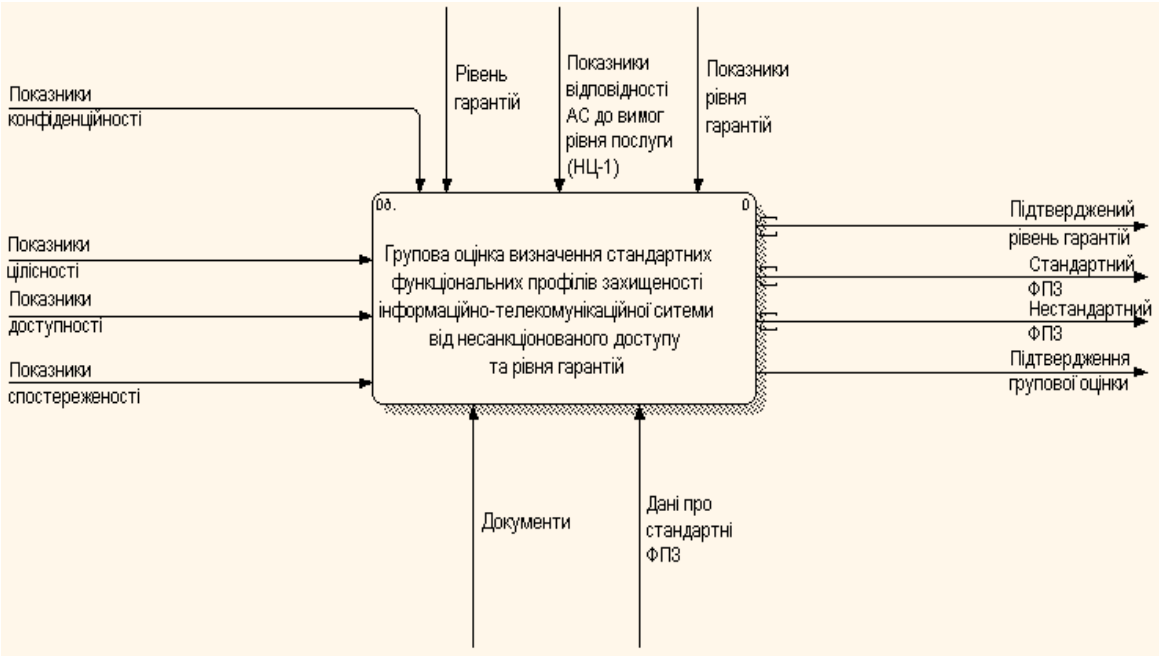


Рис. 1 - Контекстна діаграма процесу групового визначення ФПЗ та рівня гарантій

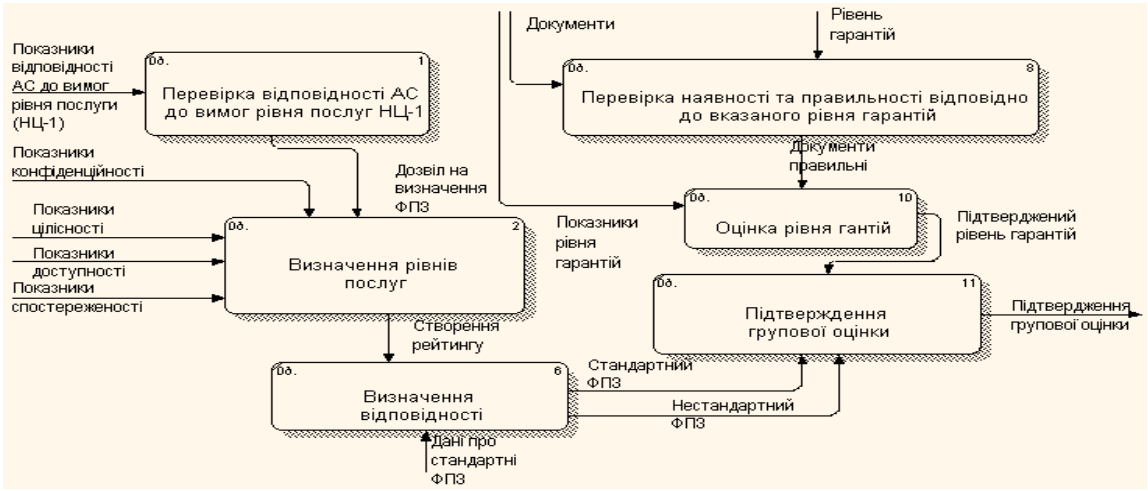


Рис. 2 - Декомпозована діаграма процесу групового визначення ФПЗ та рівня гарантій

Data Flow Diagram (DFD) – стандарт для створення моделі потоків інформації, що циркулює в ІТС. Модель системи визначається, як ієрархія діаграм потоків даних, що описують асинхронний процес перетворення інформації від введення у систему до отримання користувачем. DFD визначає, яким чином кожний процес перетворює вхідні дані у вихідні та дозволяє виявити залежності між процесами.

Діаграма включає наступні блоки: блок перевірки відповідності автоматизованої системи до вимог рівня послуги комплексу засобів захисту НЦ-1, блок отримання ФПЗ захищеності ІТС від несанкціонованого доступу, блок перевірки відповідності визначеного профілю захищеності до стандартного ФПЗ, блок визначення відповідності документів та блок оцінки рівня гарантій, блок визначення групової оцінки.

На основі нормативно-правової бази та розроблених діаграм, алгоритмів функціонування [14] було розроблено програмне забезпечення ОФПАС 2.0. Визначення функціонального профілю рис. 3 та вибір рівня гарантій рис. 4. в частині програми критерії гарантій показано на рисунках відповідно та було удосконалено даний програмний продукт визначенням групової оцінки.

Формалізація методу групового аналізу експертних оцінок при визначені рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу показано в тезах доповідей [15].

Приклад групової оцінки приведено на основі оцінки другого рівня гарантій десятьма експертами, тому наступним кроком після вибору потрібного рівня гарантій є оцінка критеріїв рис. 5 та вимог документів рис. 6 обраного рівня гарантій.

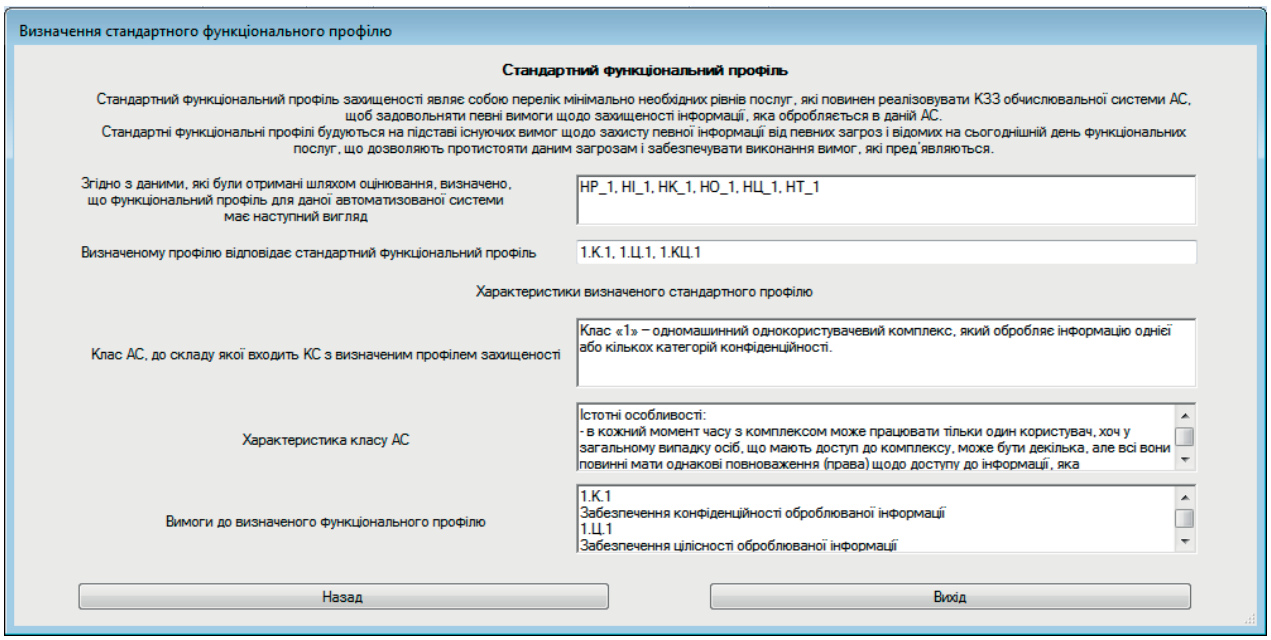


Рис. 3 - Визначення ФПЗ

Рис. 4 - Вибір рівня гарантій

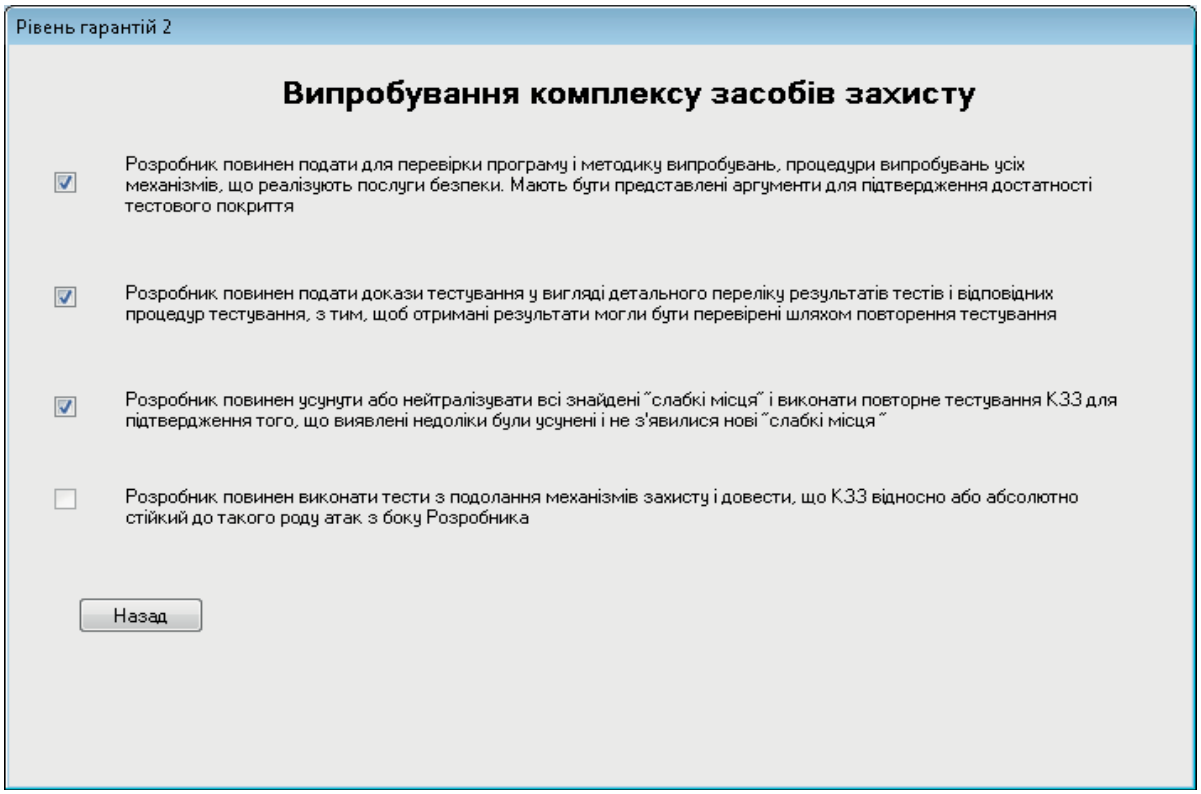


Рис. 5 - Приклад оцінки критерію

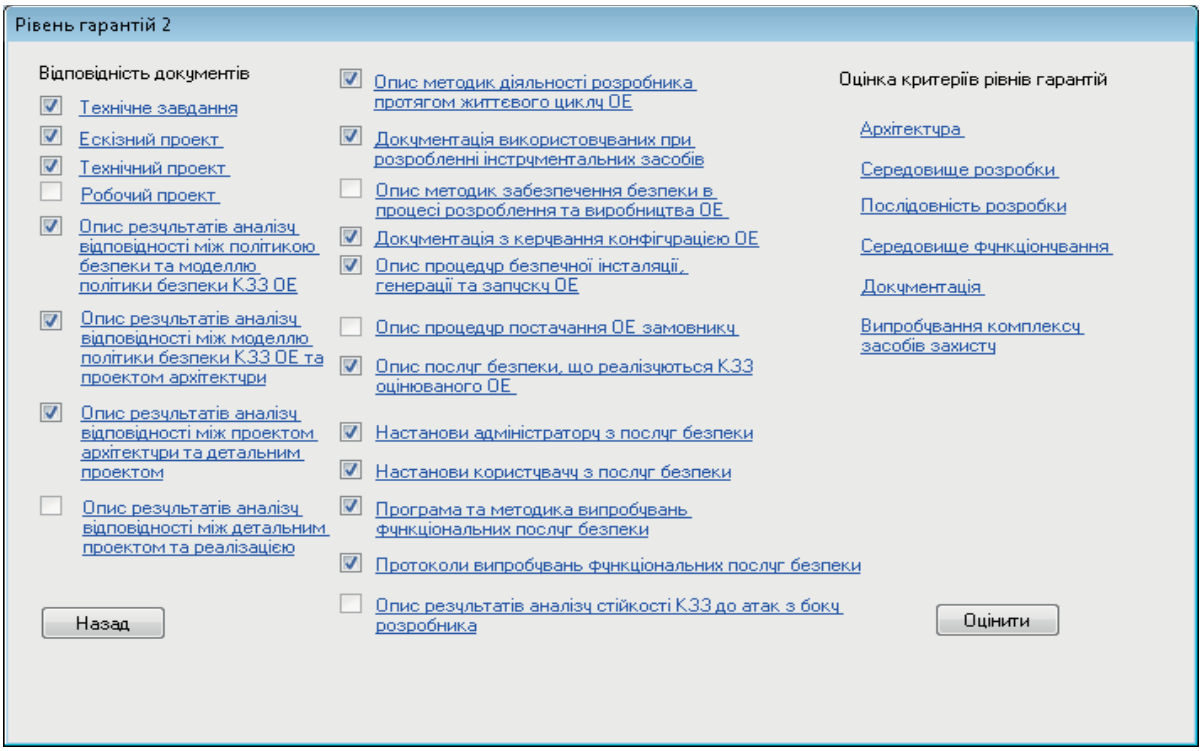


Рис. 6 - Приклад оцінки відповідності документів

Опрацювавши всі пункти експерт оцінює рівень натиснувши на кнопку «Оцінити» і перед експертом з'являється повідомлення про відповідність або не відповідність рівню гарантій. Після чого у вікні стає доступною клавіша «Відправити» для передачі отриманого результату на сервер для визначення загального результату роботи десятьох експертів рис. 7.

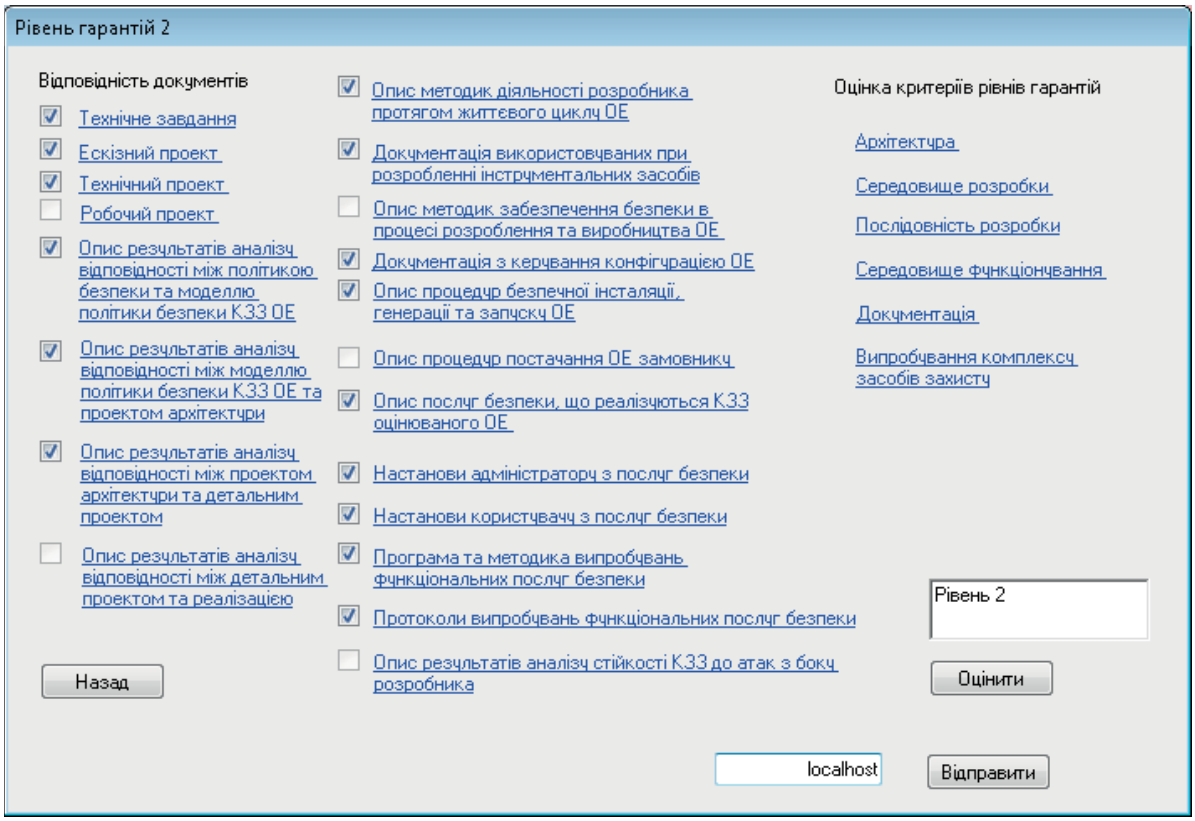


Рис. 7 - Приклад передачі результатів на сервер

Також було проаналізовано суть групової експертизи, визначено за допомогою яких методів проводиться експертиза, кількість експертів, обрано метод обробки експертної інформації [15]. Реалізацію даного методу показано на рис. 8.

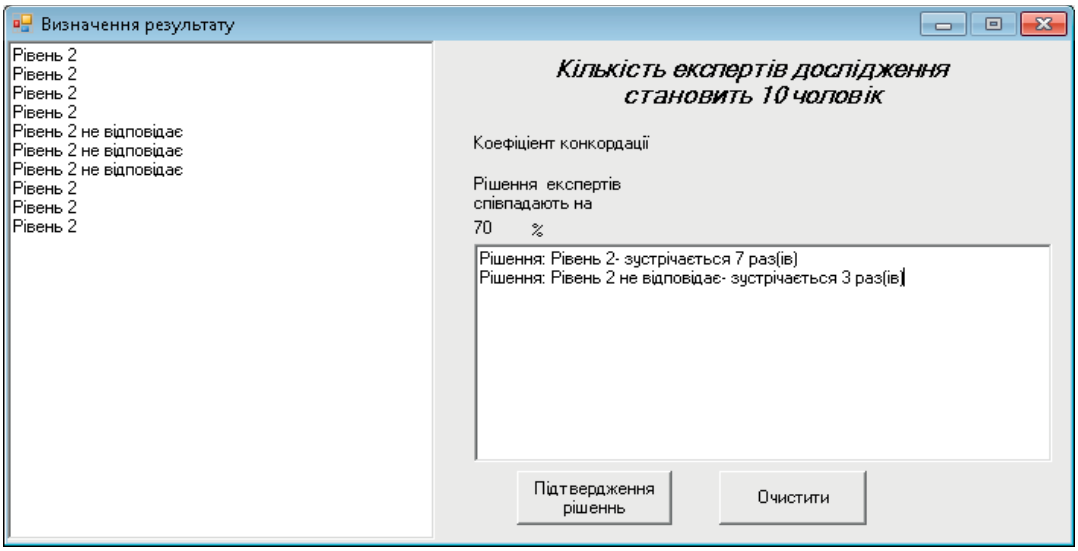


Рис. 8 - Визначення групової оцінки

5. ВИСНОВКИ

Розроблена програма дозволяє провести групову оцінку та порівняти результати відправлені на сервер. Даний підхід дозволяє зменшити час, який витрачає адміністратор безпеки для визначення функціональних профілів захищеності та рівнів гарантій оброблюваної інформації від несанкціонованого доступу, та виявити наявність співпадіння визначеного функціонального профілю із стандартним (за умови виконання даного співпадіння користувачу надається інформація про даний стандартний функціональний профіль) та підтвердити або визначити інший рівень гарантій. За рахунок проведення групової експертизи підвищується достовірність отриманих результатів.

6. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Основними результатами автори вважають здійснення реалізації групового визначення ФПЗ та рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу, яка допоможе експертній комісії швидше оцінити систему. Реалізований прототип програми дає можливість в подальшому удосконалити клієнт-серверний зв'язок програми.

7. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Юдін О. К. Державні інформаційні ресурси. Методологія побудови та захисту українського сегмента дерева ідентифікаторів / О. К. Юдін, С. С. Бучик. – К.: НАУ, 2018. – 319 с.

[2] Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99 [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41649.

[3] Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу: НД ТЗІ 2.7-010-09 [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=103247.

[4] Alimpiev, A.N., Barannik, V.V., and Sidchenko, S.A. (2017), The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. Telecommunications and Radio Engineering. 2017. Vol. 76. No 6. pp. 521-534. DOI: 10.1615/TelecomRadEng.v76.i6.60.

[5] Barannik, V. and Shulgin, S., (2016), The method of increasing accessibility of the dynamic video information resource. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET): 13th Intern. conf., (Lviv-Slavske, Ukraine, febr. 23–26, 2016). Lviv-Slavske: 2016. pp. 621-623. DOI: 10.1109/TCSET.2016.7452133.

[6] Юдін О.К. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О.К. Юдін, Р.В. Зюбіна, О.В. Фролов // Радиоэлектроника и информатика. – 2015.– № 3. – С. 13 - 21.

[7] Юдін О. К. Захист інформації в мережах передачі даних: підручник / О. К. Юдін, О.

Г. Корченко, Г. Ф. Конахович. – К. : Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 716 с.

[8] Грайворонський М. В. Безпека інформаційно-телекомунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.

[9] Потій О. В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу /О. В. Потій, А. В. Лєншин //Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2010. – Том 9. – №3. – С.479 – 488. – Режим доступу: http://openarchive.nure.ua/handle/document/410.

[10] Лєншин А. В. Метод формування функціональних профілів захищеності від несанкціонованого доступу // А. В. Лєншин, П. В. Буслов. // Радіоелектронні і комп'ютерні системи : науч. тр. – Х.: Нац. аэрокосм. ун-т "ХАИ", 2010. – Вып. 7(48). – С. 77 – 81. – Режим доступу: http://nbuv.gov.ua/UJRN/recs_2010_7_15.

[11] Берестов Д. С. Побудова парето-оптимальних функціональних профілів захищеності / Д. С. Берестов, М. О. Гульков, В. А. Козачок // Збірник наукових праць. Вип. 1(39) / Редкол. Шевченко В. Л. (голова) та ін. – К.: ЦВСД НУОУ, 2009. – С. 89 – 94. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Znpcvsd/2009_1/12.pdf.

[12] Лєншин А. В. Морфологічний метод побудови таксономії функціональних послуг захисту від несанкціонованого доступу / А. В. Лєншин // Матеріали другої міжнар. наук.-пр. конф. молодих вчених – Ч.2. – Одеса, ОНАЗ, 2012. – 133–136 с. – Режим доступу: https://onat.edu.ua/dif_files/sborniki/Zbirnyk2012_2.doc.

[13] Проценко А. А. Системный анализ профиля защищённости открытых информационных систем // А.А. Проценко, А.В. Блюма, А.Д. Кожуховский // Системи обробки інформації". – Х., 2015, 7(132) – С.128 – 131. – Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/12373/soi_2015_7_29.pdf.

[14] Бучик С.С. Формалізація методу групового аналізу експертних оцінок при визначені рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу / Бучик С.С., етребко Р.В. // Інформаційна безпека та комп'ютерні технології (INFOSEC & COMPTECH) : III міжнародна науково-практична конференція, 19 – 20 квітня 2018 року : тези доп. – Кропивницький: ЦНТУ, 2018. – С. 40-41.

[15] Бучик С.С. Реалізація програмного забезпечення визначення функціональних профілів та рівня гарантій автоматизованих систем від несанкціонованого доступу / С.С. Бучик, Р.В. Нетребко // Наукоємні технології. – 2017.– № 4 (36). – С. 309 - 315, DOI: 10.18372/2310-5461.36.12228.

Бучик Сергій Степанович, доктор технічних наук, доцент, *Зараз працює професором кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченко. Наукові інтереси: інформаційна безпека, кібербезпека, інформаційні технології, теорія прийняття рішень.*

Юдін Олександр Костянтинович, доктор технічних наук, професор, *Зараз працює професором кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченко. Наукові інтереси: інформаційна безпека, кібербезпека, інформаційні технології, теорія кодування.*

Нетребко Руслан Васильович*, закінчив Житомирський військовий інститут ім. С. П. Корольова Національного авіаційного університету, отримав освіту за спеціальністю «Системи управління та автоматики», здобув кваліфікацію інженера з керування та обслуговування систем. Наукові інтереси інформаційні технології, інформаційна безпека, кібербезпека.*

DOI: https://doi.org/10.17721/ISTS.2019.1.19-26
УДК 004.056

МЕТОД РОЗРАХУНКУ ЙМОВІРНОСТІ РЕАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ВІД ВНУТРІШНЬОГО ПОРУШНИКА

Бойченко Олег [1]
orcid.org/ 0000-0003-3048-4184

Зюбіна Руслана [2]
orcid.org/0000-0002-8654-6981

[1] м. Житомир, Житомирський військовий інституту імені С.П. Корольова, bos_2006@ukr.net
[2] м. Київ, Київський національний університет ім. Тараса Шевченка, ziubina@knu.ua

Історія статті:
Надійшла до редакції 21.07.2019
Прийнято 29.07.2019

Ключові слова:
внутрішній порушник;
інформаційна безпека;
модель загроз;
модель порушника.

Анотація: У статті проведено аналіз нормативно-правових документів, які регламентують питання захисту інформації в інформаційно-телекомунікаційній системі. За результатами проведеного аналізу сформовано мету наукового дослідження, яке полягає в удосконаленні методу розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника. Для досягнення поставленої мети були розроблені перелік загроз інформації з обмеженим доступом, які можуть надходити від внутрішнього порушника та модель внутрішнього порушника. Розроблено метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника, який має наступні етапи: визначення рівня знань внутрішнього порушника та оцінка можливості реалізації загрози; формування моделі внутрішнього порушника; формування моделі появи мотиву поведінки внутрішнім порушником; розрахунок імовірності реалізації загроз інформації з обмеженим доступом внутрішнім порушником. Проведено перевірку працездатності розробленого методу для наступних співробітників установи (організації): системний адміністратор, оператор автоматизованого робочого місця, інженер з телекомунікацій та співробітника, який не є користувачем інформаційно-телекомунікаційної системи та не належить до технічного персоналу. Результати перевірки дозволяють зробити висновок про те, що найбільш імовірна реалізація загроз інформації з обмеженим доступом від співробітників установи (організації) йде від тих співробітників, які є користувачами інформаційно-телекомунікаційної системи, мають високий рівень знань щодо можливості реалізації загроз та які мають мотив поведінки – помста. Розроблений метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника, крім загальноприйнятої класифікації рівнів можливостей, використовуваних методів і способів здійснення дій та місця здійснення дій, враховує мотив неправомірних дій з боку внутрішнього порушника та оцінку його знань щодо можливості реалізації загроз інформації з обмеженим доступом в інформаційно-телекомунікаційній системі.

Abstract: In the article analyzed regulatory documents which regulate the question of information security in the information and telecommunication system. According the results of the analysis the aim of scientific research, which consists in the improvement of method of calculation of probability of realization of threats of information with the limited access from an internal user violator was formed. To achieve this aim, a list of threats of information with limited access which could come from an internal user violator and the internal user violator model was developed. The method of calculation of probability of realization of threats of information with the limited access from an internal user violator was developed and has the followings stages: determination of level of knowledge's of internal user violator and assessment of the possibility of realizing the threat; forming of model of internal user violator; forming of model of the appearance of the motive of behavior by the internal user violator; calculation of probability of realization of threats of information with the limited access from an internal user violator. The work of the developed method has been tested for the following employees of the institution (organization): the system administrator, the operator of the automated workplace, the

telecommunications engineer and the employee who is not the user of the information and telecommunication system and does not belong to the technical personnel. The results of the verification allow conclude that the most probable realization of the threats of information with limited access from the employees of the institution (organization) comes from those employees who are users of the information and telecommunication system, have a high level of knowledge about the possibility of realizing threats and having a motive of behavior – revenge. The developed method of calculation of probability of realization of threats of information with the limited access from an internal user violator in addition to the generally accepted classification of levels of opportunities, methods used of action and place of action, takes into account the motive of wrongful acts by the internal user violator and assessment of his knowledge about the possibility of realizing the threats of information with limited access in the information and telecommunication system.

1. ВСТУП

Сьогодні на сучасному етапі розвитку інформаційних технологій, які надають змогу проводити автоматизацію процесів обробки інформації в інформаційно-телекомунікаційних системах (ІТС), особливо актуальним стає питання захисту інформації в ІТС.

Відповідно до "Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [1] для забезпечення захисту інформації в ІТС створюється комплексна система захисту інформації (КСЗІ). В цьому ж документі вказано, що організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізації системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Вимоги та порядок створення КСЗІ визначаються наступними нормативними документами системи технічного захисту інформації:

1. "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [2], в якому визначено, що для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації.

2. "Типове положення про службу захисту інформації в автоматизованій системі" [3], в якому визначено, що служба захисту інформації здійснює свою роботу з реалізації основних організаційних та організаційно-технічних заходів з створення та забезпечення функціонування КСЗІ у відповідності з Планом захисту інформації в автоматизованій системі.

Наведені документи надають методичні вказівки щодо структури та змісту Плану захисту інформації в автоматизованій системі. Одним з розділів цього Плану є розділ, у якому визначаються загрози для інформації в ІТС. На даний час немає єдиного методологічного забезпечення щодо розробки моделі загроз для інформації та моделі порушника.

З метою удосконалення існуючого методологічного забезпечення процесу розробки моделі загроз для інформації та моделі порушника, які адекватно описують процес захисту інформації в ІТС за рахунок визначення ймовірності реалізації загроз інформації в ІТС, існує потреба у розробленні методу розрахунку ймовірності реалізації загроз інформації в ІТС. Виникнення цього важливого науково-практичного завдання обумовлено існуючим протиріччям між високими вимогами до захисту інформації в ІТС та принциповою неможливістю оцінки ймовірності реалізації загроз інформації в ІТС за рахунок застосування існуючих методів оцінки інформаційних ризиків, що й визначає актуальність та своєчасність досліджень.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідженню наукових проблем захисту інформації в ІТС присвячено багато наукових праць, основним спрямуванням яких є вирішення задачі оцінювання інформаційних ризиків в ІТС.

Авторами у наукових дослідженнях [4, 5] було запропоновано розглядати загальну структуру системи захисту інформації автоматизованої системи управління технологічними процесами об'єктів критичної інфраструктури з двох компонентів: технічного та соціокультурного; а також проведено аналіз загроз захисту інформації в даній системі.

У роботі [6] авторами було описано модель порушника безпеки інформації для захищеного вузла інтернет доступу.

Результатом наукового дослідження, наведеного у роботі [7], є модель ймовірних погроз і захисту інформації в мережах загального користування, що містить у собі модель ймовірного порушника, модель об'єкта захисту, засобу захисту, а також можливі пасивні та активні канали витоку інформації.

Автори у роботі [8] навели модель реалізації загроз інформаційній безпеці вищого навчального закладу, яка ґрунтується на результатах аналізу уразливості інформаційного ресурсу.

У ряді наукових досліджень, результати яких опубліковано у наукових працях [9-16], наведені методи та способи оцінювання ризиків інформаційної безпеки в ІТС, які ґрунтуються не лише на вітчизняних нормативно-правових документах з технічного захисту інформації, але й на міжнародних стандартах у сфери інформаційної безпеки.

Таким чином, у наукових дослідженнях, які спрямовані на розв'язання наукової задачі оцінювання інформаційних ризиків в ІТС, опис моделі порушника проводиться для внутрішніх та зовнішніх джерел загроз. Але результати останніх досліджень у сфері інформаційної безпеки [17-22] свідчать про те, що найбільшу загрозу інформаційної безпеки в ІТС становлять внутрішні джерела загроз.

Розробці моделі внутрішнього порушника, яким може бути співробітник установи (організації), у відкритих джерелах на даний час не приділено належної уваги.

Тому **метою наукової роботи** є удосконалення методу розрахунку ймовірності реалізації загроз інформації з обмеженим доступом (ІзОД) від внутрішнього порушника.

Для реалізації мети були визначені наступні завдання дослідження:

розробка переліку загроз ІзОД, які можуть надходити від внутрішніх порушників;

розробка моделі внутрішнього порушника;

розробка методу розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника на основі його моделі та переліку загроз.

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Відповідно до "Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [2] під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Відповідно до "Типового положення про службу захисту інформації в автоматизованій системі" [3] основою для проведення аналізу ризиків є модель загроз для інформації та модель порушника.

У даному науково-практичному дослідженні модель загроз для ІзОД в ІТС представляє собою перелік загроз, які можуть надходити від внутрішніх порушників. Враховуючи вимоги [2] та рекомендації [3] запропоновано визначити наступні загрози ІзОД:

1. Несанкціоноване ознайомлення з ІзОД – одержання користувачем ІТС або процесом ІзОД, що міститься в об'єкті з порушенням правил розмежування доступу.

2. Неконтрольоване ознайомлення з ІзОД – одержання користувачем ІТС або процесом ІзОД, що міститься в об'єкті з порушенням прав доступу до об'єктів.

3. Випадкова модифікація ІзОД – зміна користувачем ІТС ІзОД, що міститься в об'єкті, внаслідок його недбалості, некомпетентності, неуважності та яка не має на меті нанесення збитків ІТС.

4. Навмисна модифікація ІзОД – цілеспрямована зміна користувачем ІТС ІзОД, що міститься в об'єкті, з метою нанесення збитків ІТС.

5. Випадкове знищення ІзОД – недбала, некомпетентна або неуважна дія користувача ІТС, внаслідок якої ІзОД в ІТС зникає та яка не має на меті нанесення збитків ІТС.

6. Навмисне знищення ІзОД – цілеспрямована дія користувача ІТС з метою нанесення збитків ІТС, внаслідок якої ІзОД в ІТС зникає.

7. Несанкціоноване копіювання ІзОД – копіювання ІзОД з порушенням правил розмежування доступу, внаслідок якого відбувся витік ІзОД.

8. Випадкове поширення ІзОД – розповсюдження, обнародування ІзОД користувачем ІТС шляхом порушення політики безпеки інформації в ІТС внаслідок його недбалості, некомпетентності, неуважності та яке не має на меті нанесення збитків ІТС.

9. Навмисне поширення ІзОД – цілеспрямоване розповсюдження, обнародування ІзОД користувачем ІТС шляхом свідомого порушення політики безпеки інформації в ІТС з метою нанесення збитків ІТС.

Другою складовою для проведення аналізу ризиків є модель порушника, яка повинна бути адекватна реальному порушнику для даної ІТС.

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та

теоретичні можливості, апріорні знання, час та місце дії і т.ін [2].

У межах даного наукового дослідження будуть розглядатися лише внутрішні порушники, які є співробітниками установи (організації).

1. Користувачі ІТС:

1.1 Адміністратор безпеки.

1.2 Адміністратор обчислювальної мережі.

1.3 Системний адміністратор.

1.4 Адміністратори баз даних.

1.5 Оператори АРМ.

1.6 Керівники структурних підрозділів.

1.7 Інші співробітники установи (організації).

2. Співробітники установи (організації):

2.1 Технічні співробітники, які забезпечують експлуатацію ІТС (технік-монтажник, інженер з телекомунікацій, електрик та інші).

2.2 Технічні співробітники (прибиральниці, сантехніки та інші).

2.3 Інші співробітники установи (кухар, медична сестра та інші).

Метою внутрішнього порушника є реалізація однієї або більшої кількості загроз ІзОД. Саме розрахунок імовірності реалізації загроз ІзОД від внутрішнього порушника є метою пропонованого методу, який має наступні етапи:

1. *Визначення рівня знань внутрішнього порушника та оцінка можливості реалізації загрози* проводиться за допомогою анкетування та подальшого аналізу отриманих результатів. Тематика для проведення анкетування визначається керівником установи (організації). Результатом проведення анкетування є відносна оцінка знань внутрішнього порушника щодо можливості реалізації загроз K, яку можна розрахувати за формулою:

$$K = \frac{\sum_{i=1}^{N} k_i}{N}, \qquad (1)$$

де N – кількість анкет;

$k_i = \frac{N_r}{N_\Sigma}$ – відносна оцінка знань внутрішнього користувача за i-ю анкетою;

N_r – кількість вірних відповідей в анкеті;

N_Σ – загальна кількість питань в анкеті.

2. Формування моделі внутрішнього порушника.

Внутрішній порушник має наступні рівні можливостей, які надаються їм засобами ІТС:

1. Запуск фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки ІзОД – читання (перегляд).

2. Створення і запуск власних програм з новими функціями обробки ІзОД (проектів документів) – модифікація, видалення та копіювання.

3. Створення і запуск власних програм з новими функціями обробки ІзОД (діючі документи) – модифікація, видалення та копіювання.

4. Управління функціонуванням ІТС – надання прав доступу.

5. Управління конфігурацією ІТС та політикою безпеки.

Слід зауважити, що й для співробітників установи (організації), які не є користувачами ІТС, наведені рівні можливостей також застосовуються. Це пояснюється тим припущенням, що внутрішній порушник може маскуватися під зареєстрованого користувача ІТС.

Внутрішній порушник може здійснити свої дії щодо реалізації загроз ІзОД у наступних місцях:

1. У межах контрольованої зони.

2. У межах режимного приміщення без доступу до технічних та програмних засобів ІТС.

3. У межах режимного приміщення з доступом до технічних та програмних засобів ІТС.

Внутрішні порушники можуть використовувати наступні методи і способи здійснення дій щодо реалізації загрози ІзОД:

1. Використання агентурних методів (підкуп, шантаж та інші).

2. Використання пасивних технічних засобів перехоплення інформаційних сигналів.

3. Використання штатних апаратних або програмних засобів ІТС.

4. Використання додаткових апаратних або програмних засобів ІТС.

5. Маскування під зареєстрованого користувача ІТС.

6. Використання сторонніх програмних засобів щодо управління безпекою ІТС.

Модель внутрішнього порушника наведено в таблиці 1.

В таблиці 1 наведено окремі ознаки внутрішнього порушника, які характеризують його місце, методи і способи здійснення дій, а також рівень можливостей, що надаються йому ІТС.

Імовірність реалізації загроз внутрішнім порушником за ознаками, наведеними у моделі порушника, представлена у вигляді відношення суми кількості ознак, якими характеризується внутрішній порушник до загальної кількості цих ознак:

Таблиця 1. Модель внутрішнього порушника

№	Внутрішні порушники	Рівень можливостей					Місце дії			Методи і способи дій						Σ	Імовірність реалізації загроз
		r1	r2	r3	r4	r5	a1	a2	a3	s1	s2	s3	s4	s5	s6		
1	**Користувачі ІТС**																
1.1	Адміністратор безпеки	1	1	1	1	1	1	1	1	0	0	1	1	1	1	12	0,857
1.2	Адміністратор обчислювальної мережі	1	1	1	1	1	1	0	1	0	0	1	1	1	1	11	0,786
1.3	Системний адміністратор	1	1	1	1	0	1	0	1	0	0	1	1	1	1	10	0,714
1.4	Адміністратори баз даних	1	1	1	1	0	1	0	1	0	0	1	1	1	1	10	0,714
1.5	Оператори АРМ	1	1	1	0	0	1	0	1	1	0	1	0	1	0	8	0,571
1.6	Керівники структурних підрозділів	1	1	1	0	0	1	0	1	1	0	1	0	1	0	8	0,571
1.7	Інші співробітники установи (організації)	1	0	0	0	0	1	1	1	1	1	1	0	0	0	7	0,5
2	**Співробітники установи (організації)**																
2.1	Технічні співробітники, які забезпечують експлуатацію ІТС (технік-монтажник, інженер з телекомунікацій, електрик та інші)	0	0	0	0	0	1	1	1	1	1	1	0	0	0	6	0,429
2.2	Технічні співробітники (прибиральниці, сантехніки та інші)	0	0	0	0	0	1	1	0	1	1	0	0	0	0	4	0,286
2.3	Інші співробітники установи (кухар, медична сестра та інші)	0	0	0	0	0	1	0	0	1	1	0	0	0	0	3	0,214

$$R = \frac{\sum_{i=1}^{M} r_i + \sum_{i=1}^{N} a_i + \sum_{i=1}^{L} s_i}{M + N + L}, \qquad (2)$$

де M, N, L – кількість ознак внутрішнього порушника за рівнями можливостей, що надає ІТС, місцем здійснення дії та методом (способом) здійснення дії відповідно;

r_i – ймовірність отримання внутрішнім порушником i-го рівня можливостей. Якщо рівень можливостей отримано – $r_i = 1$, в іншому випадку $r_i = 0$;

a_i – ймовірність здійснення дій внутрішнім порушником з i-го місця. Якщо дія здійснена з i-го місця – $a_i = 1$, в іншому випадку $a_i = 0$;

s_i – ймовірність здійснення дій внутрішнім порушником i-м методом (способом). Якщо дія здійснюється – $s_i = 1$, в іншому випадку – $s_i = 0$.

3. Формування моделі появи мотиву поведінки внутрішнім порушником.

Результати аналізу сучасних підходів щодо формалізованого опису внутрішнього порушника свідчать про те, що у моделі поведінки внутрішнього порушника не враховуються його ознаки, які характеризують мотиви його поведінки при здійсненні певного виду порушень політики безпеки [17-22]. Для врахування можливих мотивів дії внутрішнього порушника проведено розробку ознак за наступними групами:

1. Кар'єрне зростання.

1.1 На посаді в установі (організації) більше двох років.

1.2 Призначений на нижчу посаду в установі (організації).

2. Рівень виплат.

2.1 Підвищений (премії, підняття зарплатні).

2.2 Згідно норм.

2.3 Зменшений (штрафні санкції).

3. Кількість дисциплінарних стягнень.

3.1 Менше 2.

3.2 Від 2 до 4.

3.3 Більше 4.

За результатами аналізу мотивів дії внутрішнього порушника розроблено наступні мотиви поведінки:

1. Помста.

2. Отримання матеріальної вигоди (збагачення).

3. Самореалізація.

Модель появи мотиву поведінки внутрішнього порушника представлено у вигляді таблиці 2.

Імовірність появи мотиву неправомірної поведінки внутрішнім порушником представлена у вигляді відношення суми кількості ознак, яким він найбільш відповідає, до загальної кількості цих ознак:

$$M = \frac{\sum_{i=1}^{C} z_i + \sum_{i=1}^{J} q_i + \sum_{i=1}^{Y} d_i}{C + J + Y}, \quad (3)$$

де C, J, Y – кількість ознак внутрішнього порушника за кар'єрним зростанням, рівнем виплат та кількістю дисциплінарних стягнень відповідно;

z_i – показники кар'єрного зростання;

q_i – показники рівня виплат;

d_i – показники кількості дисциплінарних стягнень.

Таблиця 2. Модель появи мотиву

№	Мотиви поведінки	Кар'єрний зріст		Виплати			Дисципліна			Σ	Імовірність появи мотиву
		z1	z2	q1	q2	q3	d1	d2	d3		
1	Помста	1	1	0	1	1	0	1	1	6	0,75
2	Збагачення	1	0	0	1	1	1	0	0	4	0,5
3	Самореалізація	1	0	0	0	1	1	0	0	3	0,375

4. Розрахунок імовірності реалізації загроз ІзОД внутрішнім порушником.

Для оцінки можливості реалізації загроз ІзОД в ІТС з боку внутрішніх порушників враховано появу трьох подій:

А – реалізація як мінімум однієї з загроз ІзОД відповідно до знань (кваліфікації);

В – реалізація як мінімум однієї з загроз ІзОД відповідно до характеру здійснення дій;

С – поява мотиву поведінки.

Тоді ймовірність реалізації загроз ІзОД внутрішнім порушником згідно з теоремою додавання подій представлено у наступному вигляді:

$$P(A+B+C) = R + M + K - R \cdot M - \\ -R \cdot K - M \cdot K + R \cdot M \cdot K. \quad (4)$$

Перевірку працездатності розробленого методу проведено на прикладах.

Приклад 1. Розрахувати ймовірність реалізації загроз ІзОД від системного адміністратора.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,9$.

2. З таблиці 1 визначено, що $R = 0,714$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від системного адміністратора ІТС для різних мотивів поведінки, значення яких наведено в таблиці 3.

Приклад 2. Розрахувати ймовірність реалізації загроз ІзОД від оператора АРМ.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,6$.

2. З таблиці 1 визначено, що $R = 0,571$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від оператора АРМ для різних мотивів поведінки, значення яких наведено в таблиці 3.

Приклад 3. Розрахувати ймовірність реалізації загроз ІзОД від інженера з телекомунікацій.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,6$.

2. З таблиці 1 визначено, що $R = 0,429$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від інженера з телекомунікацій для різних мотивів поведінки, значення яких наведено в таблиці 3.

Приклад 4. Розрахувати ймовірність реалізації загроз ІзОД від співробітників установи (організації), які не є користувачами ІТС.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,1$.

2. З таблиці 1 визначено, що $R = 0,214$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від співробітників установи (організації), які не є користувачами ІТС, для різних мотивів поведінки, значення яких наведено в таблиці 3.

Узагальнення прикладів наведено в таблиці 3.

Таблиця 3. Узагальнення результатів прикладів

№	Співробітники/мотиви	Імовірність реалізації
1 Системний адміністратор		
	помста	0,992
	збагачення	0,986
	самореалізація	0,982
2 Оператор АРМ		
	помста	0,957
	збагачення	0,914
	самореалізація	0,893
3 Інженер з телекомунікацій		
	помста	0,943
	збагачення	0,886
	самореалізація	0,857
4 Співробітник установи (організації), які не є користувачами ІТС		
	помста	0,823
	збагачення	0,646
	самореалізація	0,375

Результати розрахунку ймовірностей реалізації загроз ІзОД від співробітників установи (організації) у приведених прикладах дають змогу зробити наступні висновки:

1. Найбільш імовірна реалізація загроз ІзОД від співробітників установи (організації) йде від тих співробітників, які є користувачами ІТС, мають високий рівень знань щодо можливості реалізації загроз.

2. Найбільш імовірна реалізація загроз ІзОД від співробітників установи (організації) йде від тих співробітників, які мають мотив поведінки – помста.

4. ВИСНОВКИ

Проведена перевірка працездатності методу розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника дозволяє зробити висновки про те, що при застосуванні запропонованого методу отримуються кількісні значення загроз ІзОД для кожного співробітника установи (організації).

Розроблений метод розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника, крім загальноприйнятої класифікації рівнів можливостей, використовуваних методів і способів здійснення дій та місця здійснення дій, враховує мотив неправомірних дій з боку внутрішнього порушника та оцінку його знань щодо можливості реалізації загроз ІзОД в ІТС.

Метод розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника може застосовуватись як на етапі проектування КСЗІ, так і під час її експлуатації.

Подальші наукові дослідження будуть спрямовані розробку математичної моделі оцінки ризику ІзОД в ІТС від внутрішніх порушників.

5. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова Кабінету Міністрів України від 29.03.2006 № 373 [Електронний ресурс]. Режим доступу: http://www.zakon.rada.gov.ua/laws/show/373-2006-%DO%BF.

[2] Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 08.11.2005 № 125 [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074.

[3] Типове положення про службу захисту інформації в автоматизованій системі. НД ТЗІ 1.4-001-2000. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04.12.2000 № 53 [Електронний ресурс]. Режим доступу: http://www.tzi.com.ua/downloads/1.4-001-2000.pdf.

[4] В. О. Хорошко, В. В. Єрмошин, М. В. Капустян, "Методика оцінки інформаційних ризиків системи управління інформаційною безпекою", *Сучасний захист інформації*, № 3, с. 95-104, 2010.

[5] С. Гончар, Г. Леоненко, О. Юдін, "Загальна модель загроз безпеці інформації АСУ ТП", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 1 (29), с. 78-82, 2015.

[6] С. Ф. Гончар, "Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом", *Захист інформації*, Том 16, № 1, с. 40-46, 2014.

[7] М. Ю. Комаров, А. В. Ониськова, С. Ф. Гончар, "Аналіз дослідження

моделі порушника безпеки інформації для захищеного вузла інтернет доступу", *Вчені записки ТНУ імені В. І. Вернадського. Серія: технічні науки*, Том 29 (68) Ч. 1 № 5, с. 138-142, 2018.
[8] А. О. Петров, "Системи захисту інформації в мережах загального користування", *Сучасна спеціальна техніка*, № 2 (25), с. 118-123, 2011.
[9] О. О. Ільїн, В. В. Вишнівський, С. О. Сєрих, "Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки", *Сучасний захист інформації*, № 1, с. 66-72, 2017.
[10] С. С. Бучик, С. В. Мельник, "Методика оцінювання інформаційних ризиків в автоматизованій системі", *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*, Вип. 11, с. 33-43, 2015.
[11] О. Г. Пузиренко, С. О. Івко, О. О. Лаврут, О. К. Климович, "Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах", *Системи обробки інформації*, Вип. 3 (128), с. 75-79, 2015.
[12] С. С. Бучик, О. К. Юдін, Р. В. Нетребко, "Теоретичні основи визначення рівня гарантій автоматизованих систем від несанкціонованого доступу", *Наукоємні технології*, № 2 (34), с. 119-125, 2017.
[13] С. С. Бучик, О. К. Юдін, *Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія*, К. : НАУ, 2015, 214 с.
[14] Р. В. Грищук, Ю. Г. Даник, *Основи кібернетичної безпеки: монографія*, Житомир: ЖНАЕУ, 2016, 636 с.
[15] Р. М. Хмелевський, "Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності", *Сучасний захист інформації,* № 4, с. 55-70, 2016.
[16] В. Н. Дереко, "Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки", *Інформаційна безпека людини, суспільства, держави,* № 2 (18), с. 16-22, 2015.
[17] Т. Ткачук, "Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз", *Підприємство, господарство і право,* № 10, с. 182-186, 2017.
[18] В. О. Панченко, "Механізм протидії інсайдерам у системі кадрової безпеки", *Науковий вісник Львівського державного університету внутрішніх справ*, №1, с. 219-227, 2018.
[19] С. Ф. Гончар, "Модель імовірних деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті інформаційної безпеки", *Наукоємні технології,* №3, с. 250-253, 2015.
[20] Ю. П. Рак, Р. Ю. Сукач, "Математична модель оцінки ризику в проектах захисту об'єктів потенційної небезпеки", *Управління проектами та розвиток виробництва*, №2(54), с. 12-17, 2015.
[21] М. Г. Романюков, "Критерії оцінки ймовірності витоку інформації через технічні канали", *Інформатика та математичні методи в моделюванні*, Том 5, № 3, с. 240–248, 2015.
[22] О. Я. Матов, В. С. Василенко, М. М. Будько, "Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-телекомунікаційних системах", *Методи захисту інформації в комп'ютерних системах і мережах*, Т. 6, № 2, с. 62-74, 2004.

Бойченко Олег Сергійович, *Вищу освіту здобув у Житомирському військовому інституті радіоелектроніки імені С. П. Корольова у 2004 році. Закінчив ад'юнктуру ЖВІ імені С. П. Корольова у 2016 році. У 2017 році захистив дисертацію на здобуття наукового ступеня кандидат технічних наук за спеціальністю "Озброєння і військова техніка".*
Посада: начальник НДЛ наукового центру ЖВІ імені С. П. Корольова.
Наукові інтереси: моделювання інформаційних систем; системи передачі даних; криптографічний захист інформації.

Зюбіна Руслана Віталіївна, *Вищу освіту здобула у Національному авіаційному університеті у 2013 році. , Зараз працює асистентом кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченко. Наукові інтереси: інформаційна безпека, кібербезпека, інформаційні технології.*

DOI: https://doi.org/10.17721/ISTS.2019.1.27-35
УДК 681.324

ПРАКТИЧНЕ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ОЦІНЮВАННЯ ЗОВНІШНІХ ВПЛИВІВ

Оксіюк Олександр [1]
orcid.org/0000-0001-9797-6015
Мирутенко Лариса [2]
rcid.org/0000-0003-1686-261X
Шестак Яніна
orcid.org/0000-0002-1703-0316 [3]

1) Київ, Київський національний університет ім. Тараса Шевченка, 24, oksiuk@ukr.net
2) Київ, Київський національний університет ім. Тараса Шевченка, myrutenko.lara@gmail.com
3) Київ, Київський національний університет ім. Тараса Шевченка,, 24, lucenko.y@ukr.net

Історія статті:
Надійшла до редакції 26.07.2019
Прийнято 31.07.2019

Ключові слова:
інформаційна система; граф завдань; алгоритм захисту, кластеризація апаратних ресурсів; кластерізація ядер процесорів; нормалізований розподіл енергії.

Анотація: *В статті була відзначена перевага інформаційних систем перед централізованими комплексами з точки зору забезпечення безпеки інфраструктури мережі, даних, що передаються, та процедур, що застосовуються у програмному середовищі комплексу. Було вказано на технічну простоту методів розширення інформаційних- систем та, відповідно, їх масштабованість. Розроблено багаторівневу схему балансування енергоспоживання та обчислювальних ресурсів інфраструктури інформаційної системи, що базується на оптимізації графу завдань. Визначено методи оцінки оптимізації графу завдань, що базуються на показниках довжини нормалізованого графу нормалізованому розподілу енергії. Результати математичного моделювання співставленні зі статистичними даними для таких методів роботи з графами завдань як обчислення за ієрархічною структурою, алгоритми розбиття графу, методи на базі алгебраїчної теорії графів, структурування типу «Diamond Dags». Аналіз проводився для таких видів розподілу як рівномірний розподіл, біноміальний розподіл, геометричний розподіл. Результати співставлення вказують на достатньо вискоку точність прогнозування на рівні математичного моделювання. У більшості випадків значення максимального відхилення, представленого у вигляді відносної похибки, між результатами моделювання та статистичними даними залишаються в межах 10%, що показує адекватність моделювання. Тим не менш, для чотирьох пар функцій довжини нормалізованого графу і нормалізованого розподілу енергії демонструють максимальне відхилення більше 10%, що вказує на необхідність доопрацювання моделі та подальших статистичних досліджень. Запропоновано використовувати при організації захисту ресурсів інформаційної системи методів кластерізації, що дозволяють побудувати прозору схему функціонування комплексу та побудувати алгоритми моніторингу.*

Abstract: *The article highlighted the advantage of information systems in front of centralized systems in terms of ensuring the security of network infrastructure, data transmitted, and procedures used in the software environment of the complex. It was pointed out the technical simplicity of the methods of expansion of information systems and, accordingly, their scalability. A multilevel energy balance scheme and computing resources of the information system infrastructure, based on the optimization of the task graph, have been developed. The methods of estimating the optimization of the graph of tasks, which are based on the indicators of the normalized graph normalized distribution of energy, are determined. The results of mathematical modeling in comparison with statistical data for such methods of working with task graphs as calculations by hierarchical structure, graph split algorithms, methods based on algebraic theory of graphs, structuring of "Diamond Dags" type. The analysis was conducted for such types of distribution as uniform distribution, binomial distribution, geometric distribution. The results of the comparison point to a sufficiently upstart prediction accuracy at the level of mathematical modeling. In most cases, the value of the maximum deviation, presented as a relative error,*

between simulation results and statistical data remains within 10%, which shows the adequacy of the simulation. Nevertheless, for the four pairs of functions of the length of the normalized graph and the normalized energy distribution, the maximum deviation is greater than 10%, indicating the need for a revision of the model and further statistical studies. It is proposed to use in organizing the protection of resources of the information system of clusterization methods, which allow to construct a transparent scheme of functioning of the complex and to construct monitoring algorithms.

1. ВСТУП

Забезпечення високого рівня безпеки інформаційної системи в сучасних умовах стає все більш складним завданням з точки зору постійного, динамічного зростання технологічної складності і розвитку інформаційного середовища.

Будуючи та експлуатуючи інформаційної системи потрібно брати до уваги забезпечення їх живучості, тобто, можливі загрози стійкості та захищеності, а особливо ті, що безпосередньо виникають за участі зовнішніх впливів. Процес оцінювання захищеності від зовнішніх впливів інформаційних систем ***є актуальним*** і потребує дослідження, у зв'язку з постійною модернізацією існуючих та появою нових інформаційних технологій та необхідністю їх функціональної безпеки від зовнішніх і внутрішніх загроз.

Метою роботи є підвищення безпеки інформаційних систем на базі запропонованої технології розроблених методів і моделей оцінювання зовнішніх впливів.

Було розглянуто та вдосконалено методику побудови графу завдань інформаційної системи, що базується на графіку запитів, а також паралелізації планування завдань та багаторівневій схеми розподілу апаратно-програмних ресурсів. Вирішено задачу оптимізації процесу кластеризації апаратних ресурсів шляхом побудови системи віртуальних машин та подальших етапів визначення екстремумів функції розміру графіка завдань та функції повного значення енергії.

При побудові сучасної інформаційної системи (ІС) слід враховувати вимоги по масштабуванню систему, а також збільшення кількості ядер $n_я$ та тактової частоти f центральних процесорів (ЦП) інфраструктури, як на рис.1. Це надає можливість для збільшення обчислювальних потужностей, організації багатопотокової архітектури, віртуалізації апаратних ресурсів та впровадження заходів по економії енергоспоживання.

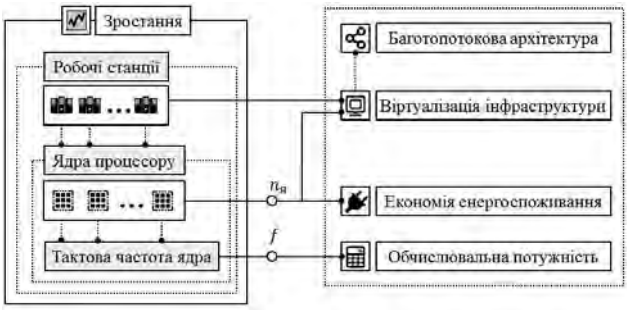


Рис. 1 - Вплив масштабування інфраструктури на можливості ІС

Підвищення продуктивності, що надається інфраструктурі ІС системою серверів на основі багатоядерних процесорів полягає у першу чергу у реалізації паралелізму процесів обробки. При цьому надається можливість запускати алгоритми багатопроцесорної обробки та втілювати принципи паралельної архітектури: суперскалярності, багатонитевості та архітектури векторних процесорів. У рамках математичного моделювання можна розглянути процес паралельних обчислень як набор n паралельних завдань з обмеженням черговості, як підмножину множини графу завдань $G(K(i), R(j))$, де $K(i)$ — набір завдань, а $R(j)$ — набір завдань з обмеженням черговості (ребра графу). При цьому i передує j, тобто $i< j$, завдання i характеризуються такими параметрами як кількість ядер $n_я$, що використовуються при виконанні завдання розміру $\mu_i \in \{\mu_1, \mu_r\}$ та набір максимальних вимог $\delta_i \in \{\delta_1, \delta_r\}$, що визначається через кількість команд, що мають бути виконані. Відповідно, робота завдання і може бути визначена як добуток $w_i = \delta_i \mu_i$.

Оцінка впливу системи розподілення навантаження на продуктивність роботи ІС.

Багатоядерність процесорів надає широкі можливості по оптимізації роботи обчислювальної системи та координуванню навантаження, як обчислювальних ресурсів, так і електронного вантаження [11-15]. Слід зауважити, що обчислювальна потужність багатоядерного процесору з числом ядер $n_я$ наближається до значення потужності $n_я$ одноядерних процесорів, або потужності одного

одноядерного процесору з $n_я$ разів більшою частотою. Але при цьому рівень електроенергії яка необхідна для його роботи E_n складає менше значення ніж рівень електроенергії, що використовується одноядерним процесором з більшою тактовою частотою:

$$E_n = \frac{E_1}{n_я^{\sigma}} \ , \qquad (1)$$

де параметр залежить від особливостей побудови багатоядерного процесору і лежить у таких межах:

$$\left\{ \begin{array}{c} \sigma \in N \ \{\backslash displaystyle \ \backslash mathbb\{N\}\} \\ \sigma > 1 \end{array} \right\} \qquad (2)$$

При належній організації роботи ІС на основі багатоядерних серверів з'являється можливість суттєво підвищити продуктивність обробки запитів системою, що базується на розпаралелюванні роботи. При паралельній архітектурі ІС взаємодія між ядрами може здійснюється через передачу даних і через спільну пам'ять, а ступінь паралелізму, таким чином, збільшується зі збільшенням числа ядер. Це відкриває широкі можливості для створення мультизадачних алгоритмів, а отже обробки значної запитів користувачів на одиницю часу. У разі виконання ІС значної кількості паралельних запитів головним завданням стає виділення ядер для кожного завдання, створення, так званого, графіку завдань, що забезпечує балансування навантаження на апаратні ресурси і оптимальний рівень споживання електроенергії [6-10].

Графік завдань є сучасним засобом побудови алгоритмів роботи ІС. Згідно даної моделі запити, що знаходять на різних рівнях системи вважаються незалежними, і тому для їх вирішення можуть бути використані типові алгоритми. Це певною мірою обмежує інструментарій розробки ІС, але при цьому допомагає проблему обмеження черговості при плануванні завдань і спрощує аналіз системи [7, 8]. Іншим засобом є кластеризація апаратних ресурсів ІС. У рамках даної архітектури кожне завдання надає запит до кількох ядер, тому виникає необхідність розділення ядер процесора на кластери. Крім того схема враховує механізм організації розподілу ресурсів, тобто визначення оптимальних пропорцій при наданні для окремого завдання апаратних ресурсів з метою забезпечення надійної роботи при обробці запитів, що було розглянуто у попередньому підрозділі.

Проектування ІС починається з розподілу для ЦП серверів електроенергії, рівень якої визначається через величину:

$$P = \eta \left(f \times CU^2 \right) \qquad (3)$$

де η – коефіцієнт використання ЦП, f – тактова частота, C – ємність навантаження, U – напруга живлення.

Слід зауважити, що дані параметри не є незалежними, так, наприклад напруга живлення є функцією від частоти:

$$U = b f^{(\sigma+1)}, \qquad (4)$$

де b є константою, що визначається окремо для кожного типу багатоядерного процесору.

Наступним кроком при розробці ІС є визначення швидкодії роботи ЦП, що також залежить від тактової частоти f та параметру, що характеризує процесор d:

$$S = df \qquad (5)$$

Отже, показник споживання електроенергії ЦП серверів ІС може бути визначено як:

$$P = \eta b^2 C f^{2\sigma+3} \qquad (6)$$

що можна спростити до вигляду:

$$P = \beta s^{\alpha} \qquad (7)$$

де $\left\{ \begin{array}{c} \alpha = 2\sigma + 3 \\ \beta = \eta b 2\, C / d\alpha \end{array} \right.$ (8)

При обробці r паралельних запитів, завдання з обмеженням черговості є підмножиною множини графу завдань. За схемою, що буде розглянута у даній роботі виконання завдання j слідує за виконанням завдання i. Всі завдання і при цьому виконуються паралельно і характеризуються наступним набором параметрів [6-10]:

- кількість ядер ЦП серверів, що використовуються при виконанні завдання μ_i;
- максимальний рівень вимог до обчислювальних потужностей ядер δ_i, що

визначається через кількість команд, що мають бути виконані при обробці запиту;

- робота завдання $w_i = \mu_i \delta_i$.

Швидкодія обробки запиту і потужність, що надається для його виконання можуть бути пов'язані через параметр α:

$$P_i = S_i^{\alpha} \tag{9}$$

а час обробки запиту через параметр:

$$t_i = \frac{\delta_i}{S_i} => t_i = \frac{\delta_i}{\sqrt[\alpha]{P_i}} \tag{10}$$

У випадку коли система складається з однакових ЦП, що при балансуванні навантаження працюють з однією швидкістю S_i протягом одного t_i, електроенергія, яка витрачається на запит і множини *[1,r]* визначається наступним чином:

$$e_i = \mu_i P_i t_i => e_i = w_i S_i^{\alpha-1} \tag{11}$$

Таким чином, процес оптимізації ІС при цьому складається з двох базових етапів [17, 18]:

- етап побудови графіка завдань, що характеризується найменшим розміром, з урахування обмеження на величину повної енергії E_Σ;
- визначення мінімуму функції повної енергії E_Σ, з урахуванням обмежень на розмір графіка завдань.

При цьому, на першому етапі за основу береться множина розміру завдань $\mu_i \in \{\mu_1, \mu_r\}$ та множина вимог $\sigma_i \in \{\sigma_1, \sigma_r\}$, а для другого множина значень потужностей $p_i \in \{p_1, p_r\}$, як показано на Рис. 2.

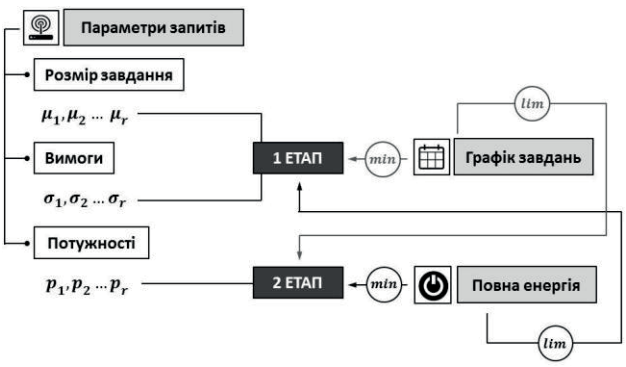


Рис. 2 - Оптимізація роботи ІС через створення графіку завдань

Оптимальне значення розміру графіка завдань *G_min* може бути визначено через значення повної роботи *W*:

$$T^{min} \geq n_я \left(W^{\alpha} / E\right)^{\frac{1}{\alpha-1}}, \tag{12}$$

а оптимальне значення функції повної енергії у такому разі, відповідно визначається як:

$$E_\Sigma^{min} \geq W^{\alpha} (n_я T)^{1-\alpha}, \tag{13}$$

де повний об'єм роботи для r паралельних запитів, обчислюється як:

$$W = \sum_{i=1}^{r} w_i => W = \sum_{i=1}^{r} \mu_i \delta_i \tag{14}$$

Узагальнення математичної моделі розподілення навантаження на апаратні ресурси ІС включає у себе побудову системи багатоядерних процесорів з $n_{я-i}$ ідентичними ядрами у кожному. При цьому можна побудувати графік роботи x алгоритмів, що виконуються паралельно, яким відповідає набір графів завдань $G_i \in \{G_1, G_x\}$ та багатоядерні процесори $P_i \in \{P_1, P_y\}$ з кількістю ядер у кожному $n_{я-i} \in \{n_{я-1}, n_{я-y}\}$, відповідно [11-16]. Оптимізація полягає у тому, щоб для r паралельних завдань розміру $\mu_i \in \{\mu_1, \mu_r\}$, що характеризуються вимогами $\delta_r \in \{\delta_1, \delta_r\}$ отримати мінімальний розмір графіка завдань T^{min} (рівняння 12) через обрахування множини робот завдань $\{w_1 \dots w_r\}$. При цьому слід врахувати обмеження на повне значення енергії системи та мінімум функції енергії E_Σ^{min} (рівняння 12). Також для множини $\{p_1 \dots p_r\}$ необхідно визначити мінімум функції енергії E_Σ^{min}, з урахуванням обмеження на розмір графіка завдань T; оптимальні параметри роботи ІС отримуються при співставленні цих значень, що можуть бути обраховані через наступну систему рівнянь:

$$\begin{cases} T^* \geq \sqrt[\alpha-1]{\dfrac{n_я}{E}\left(\dfrac{\sum_{i=1}^{r} w_i}{n_я}\right)^{\alpha}} \\ E^* \geq n_я \dfrac{\left(\sum_{i=1}^{r} w_i / n_я\right)^{\alpha}}{T^{\alpha-1}} \end{cases} \quad (15)$$

Як було вказано ребра графу завдань мають будуватися таким чином, що для вузлів *i* та *j* — $i < \mathrm{j}$, де *i* попередник *j*. Додатковою умовою є те, що якщо існує вузол *k*, для якого можна знайти ребра (i,k) та (k,j), то ребро (i,j) виключається з графу, тобто графу завдань є направленим ациклічним графом, який може бути розкладено на y рівнів $l \in \{1 \ldots y\}$.

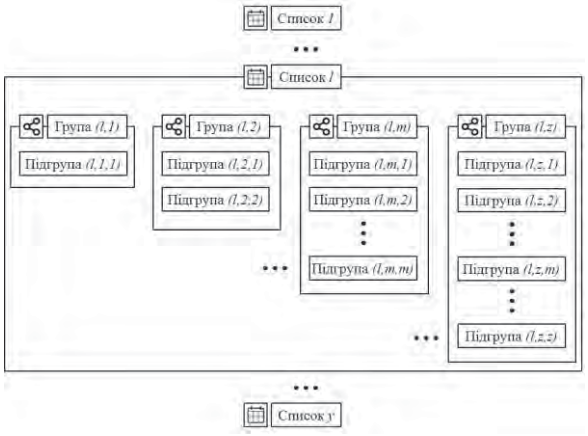


Рис.3 - Структурування графіку завдань на рівні списків, груп і підгруп

Завдання i знаходиться на рівні l^+, якщо кількість вузлів від даного завдання до початкового завдання по найдовшому шляху складає величину l^+. При цьому всі завдання, які знаходяться на одному рівні виконуються незалежно один від одного. Список незалежних паралельних завдань (рис. 3) на рівні l поділяється на z груп $(l,1) \ldots (l,m) \ldots (l,z)$. Таким чином, для величини $m \in [1, z-1]$, можна отримати групу (l,m), що характеризується розміром $\mathrm{n}_{я-i}$ (по кількості ядер), який лежить у межах:

$$\frac{n_я}{m+1} < \mathrm{n}_{я-i} \leq \frac{n_я}{m} \quad (16)$$

Така система ефективно працює з великим набором завдань мінімального розміру, що є типовим для сучасних ІС. На її основі можна побудувати алгоритми, що поділяють $n_я$ ядер на m кластерів, кожен з яких містить $n_я/m$ ядер. Кожен окремий кластер обслуговує одне завдання групи (l,m), де не паралельні завдання кількістю $n \leq m$ виконуються одночасно.

Планування паралельних завдань групи (l,m) на m кластерах, кожне завдання якого характеризується множиною розміру завдань $\mu_i \in \{\mu_1, \mu_r\}$ та набором максимальних вимог $\delta_i \in \{\delta_1, \delta_r\}$ може бути представлено як побудова списку послідовних завдань на m процесорах, де кожне завдання характеризується максимальними вимогами до процесору (без врахування енерговитрат, див. рівняння 1-2). Якщо багатоядерний процесор з $n_я$ ядрами розбито на m кластерів, у рамках виконання завдань з групи (l,m) дана група поділяється на підгрупи завдань $\{(l,m,1) \ldots (l,m,m)\}$, причому кожна з зазначених підгруп виконується на одному кластері.

Зазначений етап розрахунку оптимальних значень енергії та розміру графіка завдань виконується після етапу кластеризації ядер процесорів. Таким чином, процес графу завдань здійснюється шляхом визначення часу виконання завдань *i* за допомогою параметрів з набору максимальних вимог δ_i. Алгоритм планування списку у такому разі складатиметься з наступних етапів [11-16]:

1. Окрема задача *k* має бути розподілена по відношенню до кластеру $k \in [1, m]$;

2. Перше позапланове завдання списку $(m+1)$ видаляється зі списку і включається для виконання до кластеру;

3. Перехід до пункту (1) з повторенням процесу до завершення повного набору процесів списку.

У таблиці вказано повний набір алгоритмів, що базуються на значеннях розміру завдання $\mu_i \in \{\mu_1, \mu_r\}$, набору максимальних вимог $\delta_i \in \{\delta_1, \delta_r\}$ та роботи завдання w_i, що можуть бути використані при упорядкуванні складових графу завдань.

Розділення потужностей ІС за напрямками, специфікою роботи, та оцінка підвищення ефективності виконання завдань ІС внаслідок здійснення такого розподілення.

Поділення складових графу завдань ІС на списки, групи та підгрупи дозволяє розробити оптимальну схему розподілу енергії та

обчислювальної потужності апаратних ресурсів інфраструктури.

Таблиця 1. Схеми організації списку планування за ключовими параметрами

Параметр	Назва	Принцип
Розмір завдання	SRF: Smallest Requirement First	$\delta_1 \le \delta_2 \le \ldots \le \delta_n$
	LRF: Largest Requirement First	$\delta_1 \ge \delta_2 \ge \ldots \ge \delta_n$
Максимальні вимоги	SSF: Smallest Size First	$\mu_1 \le \mu_2 \le \ldots \le \mu_n$
	LSF: Largest Size First	$\mu_1 \ge \mu_2 \ge \ldots \ge \mu_n$
Робота по виконанню завдання	SWF: Smallest Work First	$w_1 \le w_2 \le \ldots \le w_n$
	LWF: Largest Work First	$w_1 \ge w_2 \ge \ldots \ge w_n$

Паралельні задачі розкладаються на y рівнів, завдання на кожному рівні l поділяються z груп $\{(l,1)\ldots(l,z)\}$, а завдання у кожній групі m поділяються на z підгруп $\{(l,m,1)\ldots(l,m,m)\}$. Таким чином, оптимальна схема розподілу потужності може бути визначена через обмеження довжини графу або енергоспоживання в межах, як груп так і підгруп, що дозволяє побудувати чотири рівні [11-16] аналізу (рис. 4):

1. Оптимізація розподілу апаратних ресурсів РІТС у межах однієї підгрупи завдань;
2. Оптимізація розподілу апаратних ресурсів РІТС на рівні взаємодії між підгрупами завдань;
3. Оптимізація розподілу апаратних ресурсів РІТС на рівні взаємодії між групами завдань;
4. Оптимізація розподілу апаратних ресурсів РІТС на рівні взаємодії між списками завдань.

Реалізація схеми оптимізації для першого рівня є найпростішим у реалізації етапом.

Виконання завдань у межах підгрупи здійснюється послідовно, довжина списку завдань підгрупи мінімізується при відповідних значеннях p_i і T [11-16]:

$$\begin{cases} p_i = \dfrac{\sqrt[\alpha-1]{\sum_i E_i^{\alpha} \div \sum_i \mu_i \delta_i^{\alpha}}}{\mu_i} \\ T = \sqrt[\alpha-1]{\dfrac{\sum_i \mu_i \delta_i^{\alpha}}{E_i}} \end{cases} \quad (16)$$

Відповідно на другому рівні розглядається взаємодія між підгрупами завдань. При цьому $n_я$ ядер розділяється на m кластерів, причому кожен кластер утримує $n_я / m$ потужності.

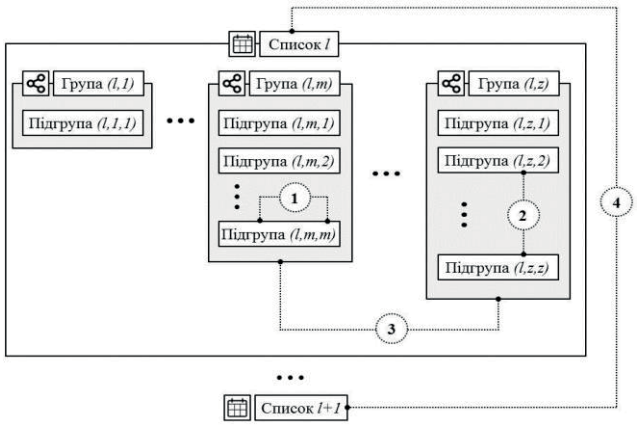


Рис. 4 - Багаторівнева схема оптимізації розподілу апаратних ресурсів ІС

Кожен кластер розглядається як окремий елемент призначений для обробки окремої задачі, відповідно повний набір задач поділяється на m підгруп, отже кожне завдання підгрупи k виконується кластером k. Оптимальні значення p_i, E і Tможуть бути визначені аналогічно до рівняння (17) як:

$$\begin{cases} p_i = \dfrac{\sqrt[\alpha-1]{\sum_i E_{k|i}^{\alpha} / \sum_i \mu_{k|i} \delta_{k|i}^{\alpha}}}{\mu_i} \\ E_k = \dfrac{E \sum_i \mu_{k|i} \delta_{k|i}^{\alpha}}{\sum_j (\sum_i \mu_{j|i} \delta_{j|i}^{\alpha})} \\ T = \sqrt[\alpha-1]{\dfrac{\sum_i \mu_{k|i} \delta_{k|i}^{\alpha}}{E}} \end{cases} \quad (18)$$

На третьому рівні оптимізація завдань здійснюється для всіх z груп окремого списку, причому у відповідності до правил розбиття

кожна j група утримує i підгруп, причому $i = j$. Значення T у відповідності до (рівняння 18) можна записати як [11-16]:

$$T = \sqrt[\alpha-1]{\frac{\sum_i \mu_{j|i} \delta_{j|i}^{\alpha}}{E_J}} \quad (19)$$

Зменшення T відбувається через оптимальній розподіл E_j

$$\begin{cases} E_j = \left(\frac{\sqrt[\alpha]{\sum_j \mu_{j|i} \delta_{j|i}^{\alpha}}}{\sum_i \sqrt[\alpha]{\sum_j \mu_{j|i} \delta_{j|i}^{\alpha}}} \right) E \\ T = \sqrt[\alpha-1]{\frac{\sum_i \sum_j \mu_{j|i} \delta_{j|i}^{\alpha}}{E}} \end{cases} \quad (20)$$

Відповідно, при оптимізації розподілу апаратних ресурсів ІС на рівні взаємодії між списками завдань (четвертий рівень) ми переходимо до $l \in [1, y]$ списків завдань. Значення T аналогічно до виразу (20) розраховується як:

$$T = \sum_l \frac{\sum_i \sqrt[\alpha]{\mu_{l|j|i} \delta_{l|j|i}^{\alpha}}}{\sqrt[\alpha-1]{E_l}} \quad (21)$$

На четвертому рівні зменшення T аналогічно до виразу (21) відбувається через оптимальній розподіл E_l:

$$\begin{cases} E_l = \left(\frac{\sum_j \sqrt[\alpha]{\sum_i \mu_{l|j|i} \delta_{l|j|i}^{\alpha}}}{\sum_i \sum_j \sqrt[\alpha]{\sum_i \mu_{l\setminus j\setminus i} \delta_{l\setminus j\setminus i}^{\alpha}}} \right) E \\ T = \sqrt[\alpha-1]{\frac{\sum_l \sum_j \sum_i \mu_{l|j|i} \delta_{l|j|i}^{\alpha}}{E_l}} \end{cases} \quad (22)$$

У такому разі довжина нормалізованого графа завдань (NSL: Normalized Schedule Length) може бути визначена відповідно до [15] як:

$$NSL = n_я \left(\frac{\sum_l \sqrt[\alpha]{\sum_j \sum_i \mu_{l|j|i} \delta_{l|j|i}^{\alpha}}}{W} \right)^{\frac{\alpha}{\alpha-1}} \quad (23)$$

Відповідно нормалізований розподіл енергії (NEC: Normalized Energy Consumption) обраховується згідно [14] як:

$$NEC = n_я^{\alpha-1} \frac{\left(\sum_l \sqrt[\alpha]{\sum_j \sum_i \mu_{l|j|i} \delta_{l|j|i}^{\alpha}} \right)^{\alpha}}{W} \quad (24)$$

Для верифікації даних підходів було проведено моделювання зазначеної схеми для типових методів роботи з графами завдань [15]:

- обчислення за ієрархічною структурою;
- алгоритми розбиття графу (Partitioning Algorithms);
- методи на базі алгебраїчної теорії графів (Linear Algebra Task Graphs);
- структурування типу «Diamond Dags».

Отримані результати математичного моделювання були надалі співставленні зі статистичними даними [14], що були визначені для наступних видів розподілу:

- рівномірний розподіл;
- біноміальний розподіл;
- геометричний розподіл.

Результати співставлення представлені на рис. 5 — 6. Вони вказують на достатньо високу точність прогнозування на рівні математичного моделювання.

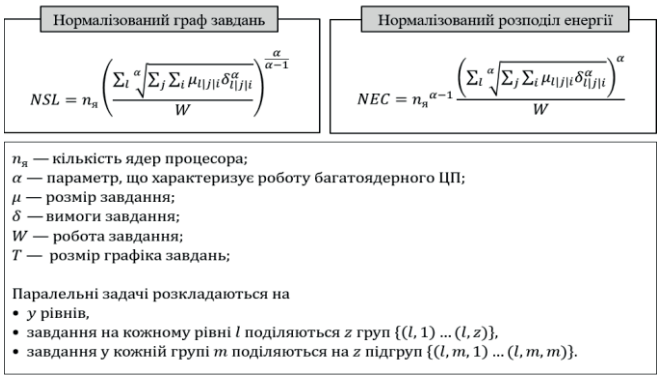


Рис. 5 – Результати математичного моделювання

Наведені графіки залежностей вказують подібність залежностей для різних методів роботи з графами при роботі з одним типом розподілу при різних абсолютних значеннях NEC та NSL, що доводить ефективність розробленого підходу для широкої групи методів.

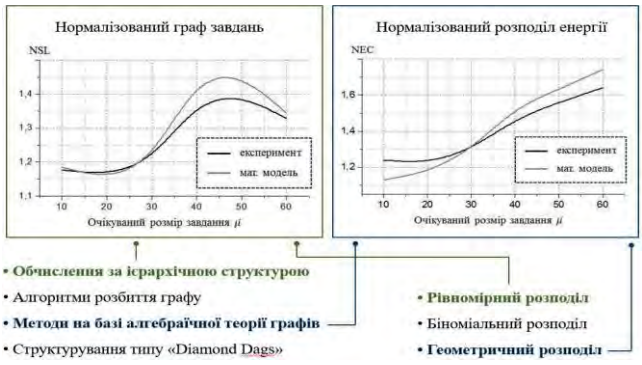


Рис. 6 – Результати графіків залежностей

6. ВИСНОВОК

Розглянуто та вдосконалено методику побудови графу завдань інформаційної системи, що базується на графіку запитів, а також паралелізації планування завдань та багаторівневій схеми розподілу апаратно-програмних ресурсів. Вирішено задачу оптимізації процесу кластеризації апаратних ресурсів шляхом побудови системи віртуальних машин та подальших етапів визначення екстремумів функції розміру графіка завдань та функції повного значення енергії.

7. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Gupta, H. Load "Balancing In Cloud Computing," *International Journal of Recent Trends in Engineering and Research,* Vol. 3(3), pp. 260-267, 2017.

[2] S. Kaur, T. Sharma, "Efficient load balancing using improved central load balancing technique," in *Proceedings of the 2nd International Conference on Inventive Systems and Control (ICISC)* 2018.

[3] S. Pandey, "Cloud Load Balancing: A Perspective Study," *International Journal Of Engineering And Computer Science*, Vol. 6, Issue 6, pp. 21602-21611, 2017

[4] R. Podaralla, "Balancing Load in Smartphone's," *International Journal Of Engineering And Computer Science*," Vol. 6, Issue 1, pp. 19987-19983, 2017.

[5] P. Membrey, D. Hows, E. Plugge, *Load Balancing Basics*, in: Practical Load Balancing, Apress, 2012, pp. 109-116.

[6] W. N. Ariffin, S. Salleh, "The matching technique of directed cyclic graph for task assignment problem," in *Proceedings of the International Conference on Quantitative Sciences and Its Application,* At Langkawi, 2014, pp. 387-394.

[7] Ariffin, W. N., & Salleh, S. "Bi-partition approach of directed cyclic task graph onto multicolumn processors for total completion time minimization task assignment problem," in *Proceedings of the 2nd International Conference on Mathematics,* Engineering and Industrial Applications 2016, Songkhla; Thailand, 2016.

[8] C. Yang, C. Lin, "Time-Varying Network Measures in Resting and Task States Using Graph Theoretical Analysis," *Brain Topography*, Vol. 28, Issue 4, pp. 529-540, 2015.

[9] Y. Masoudi, S. Lotfi, D. Karimzadgan, F. Fathy, K. Abdi, "Static Task Graph Scheduling in Real Time Homogenous Multiprocessor Systems Using Learning Automata," in *Proceedings of the 2011 International Conference on Communication Systems and Network Technologies*, Katra, Jammu, 2011, pp. 423-429.

[10] Yang, C., & Lin, C. (2015). Time-Varying Network Measures in Resting and Task States Using Graph Theoretical Analysis. Brain Topography, 28(4), 529-540.

[11] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, 2010.

[12] K. Li, "Performance analysis of power-aware task scheduling algorithms on multiprocessor computers with dynamic voltage and speed," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 11, pp. 1484–1497, 2008.

[13] K. Li, "Energy efficient scheduling of parallel tasks on multiprocessor computers," *Journal of Supercomputing,* vol. 60, no. 2, pp. 223–247, 2012.

[14] K. Li, "Power allocation and task scheduling on multiprocessor computers with energy and time constraints," in: Y. Zomaya and Y. C. Lee (Eds.), Energy-Efficient Distributed Computing Systems, A., Chapter 1, John Wiley & Sons, 2012, pp. 1-37.

[15] S. U. Khan, *Handbook on Data Centers,* New York, NY: Springer, 2015, 369 p.

[16] K. Li, "Algorithms and analysis of energy-efficient scheduling of parallel tasks," in: I. Ahmad and S. Ranka, (Eds.), Handbook of Energy-Aware and Green Computing, Vol. 1 (Chapter 15), CRC Press/Taylor & Francis Group, 2012, pp. 331-360.

Оксіюк Олександр Глібович, *д.т.н., професор, завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Основними напрямками наукових досліджень є фундаментальні та прикладні дослідження, пов'язані з розвитком інтелектуальних систем, логіко-лінгвістичного моделювання в кіберпросторі, теорії та практики розробки автоматизованих систем та проведення експертних оцінок, моделей та методів побудови інтегрованої інформаційної безпеки.*

Мирутенко Лариса Вікторівна*, к.т.н., асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. У 2017 році отримала науковий ступінь кандидата технічних наук за спеціальністю "Інформаційні технології". Основними напрямками наукових досліджень є системи технічної захисту інформації, кібербезпека.*

Шестак Яніна Володимирівна*, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Основними напрямками наукових досліджень є процес оцінювання захищеності від зовнішніх впливів інформаційних систем.*

DOI: https://doi.org/10.17721/ISTS.2019.1.36-41
UDC 681.3.06

MODELING OF INFORMATION SECURITY SYSTEM IN COMPUTER NETWORK

Bogdan Korniyenko [1]
orcid.org/0000-0002-2521-0878

Liliya P. Galata [2]
orcid.org/0000-0002-7978-3954

[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine, bogdanko@i.ua
[2] National Aviation University", Kyiv, Ukraine, galataliliya@gmail.com

Paper history:
Received 17.06.2017
Accepted 25.07.2017

Keywords:
model;
modeling;
simulation;
security;
threats.

Abstract: *This article presents simulation modeling process as the way to study the behavior of the Information Security system. Graphical Network Simulator is used for modeling such system and Kali Linux is used for penetration testing and security audit. To implement the project GNS3 package is selected. GNS3 is a graphical network emulator that allows you to simulate a virtual network of more than 20 different manufacturers on a local computer, connect a virtual network to a real one, add a full computer to the network, Third-party Applications for network packet analysis are supported. Depending on the hardware platform on which GNS3 will be used, it is possible to build complex projects consisting of routers Cisco, Cisco ASA, Juniper, as well as servers running network operating systems. Using modeling in the design of computing systems, you can: estimate the bandwidth of the network and its components; identify vulnerability in the structure of computing system; compare different organizations of a computing system; make a perspective development forecast for computer system; predict future requirements for network bandwidth; estimate the performance and the required number of servers in the network; compare various options for computing system upgrading; estimate the impact of software upgrades, workstations or servers power, network protocols changes on the computing system. Research computing system parameters with different characteristics of the individual components allows us to select the network and computing equipment, taking into account its performance, quality of service, reliability and cost. As the cost of a single port in active network equipment can vary depends on the manufacturer's equipment, technology used, reliability, manageability. The modeling can minimize the cost of equipment for the computing system. The modeling becomes effective when the number of workstations is 50-100, and when it more than 300, the total savings could reach 30-40% of project cost.*

Анотація: *У статті розглянуто процес імітаційного моделювання, як спосіб дослідження поведінки системи інформаційної безпеки. Для моделювання такої системи використовується Graphical Network Simulator, а для тестування проникнення та аудиту безпеки використовується Kali Linux. Для реалізації проекту обрано пакет GNS3. GNS3 – це графічний емулятор мережі, який дозволяє моделювати віртуальну мережу з мережевого обладнання більше ніж 20 різних виробників на локальному комп'ютері, приєднувати віртуальну мережу до реальної, додавати в мережу повноцінний комп'ютер, підтримується сторонні програми для аналізу мережевих пакетів. Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережевих операційних систем. Використовуючи моделювання при проектуванні обчислювальних систем, можна: оцінити пропускну здатність мережі та її складових; виявити вразливості в структурі обчислювальної системи; порівнювати різні варіанти проектування обчислювальної системи; скласти перспективний план розробки комп'ютерної системи; прогнозувати вимоги до пропускної здатності мережі; оцінювати продуктивність і необхідну кількість серверів у мережі; порівняти різні варіанти модернізації обчислювальної системи; оцінити вплив оновлення програмного забезпечення, робочих станцій, серверів, зміни мережних протоколів на обчислювальну систему. Дослідження параметрів обчислювальної системи*

з різними характеристиками окремих компонентів дозволяє вибрати мережу і обчислювальну техніку, враховуючи її продуктивність, якість обслуговування, надійність і вартість. Оскільки вартість одного порту в активному мережному обладнанні може змінюватися в залежності від виробника, використовуваної технології, надійності, керованості. Моделювання може мінімізувати вартість обладнання для обчислювальної системи. Моделювання стає ефективним, коли кількість робочих станцій становить 50-100, а при більш ніж 300 - загальна економія може досягати 30-40% від вартості проекту.

1. INTRODUCTION

Efficient construction and usage of corporate information systems has become an extremely important task, especially in insufficient funding of information technology in enterprises. Evaluation criteria for efficiency are the cost reducing of the information system implementation, current and nearest future requirements compliance, the opportunity and the cost of further development and transition to new technologies.

The information system core is a computing system that includes next components: cable network and active network equipment, computer and peripheral equipment, data storages (libraries), system software (operating systems, database management systems), special software (monitoring and network management) and in some cases the applied software.

Two main types of computer network modeling can be considered: analytical and simulation modeling [1].

Analytical models of networks are built on the basis of mathematical tools of queuing theories, probability and Markov processes, as well as methods of diffuse approximation [1]. Also, as methods of analytical network modeling, differential and algebraic equations can be used that describe the network behavior in time.

When using analytical modeling, it is often possible to obtain models for solving a fairly wide range of computer network research tasks. At the same time, analytical network models have a number of significant drawbacks, which include:

- significant simplifications inherent in most analytical models (such simplifications sometimes call into question the results of analytical modeling);
- cumbersome calculations for complex models.

Thus, despite the significant achievements of analytical modeling, many real-life situations cannot be adequately represented using appropriate mathematical models. In some cases, this is hampered by a certain "rigidity" of mathematics as a language for describing and representing events and phenomena. In other cases, even if it is possible to formalize the life situation under consideration through the construction of a mathematical model, the optimization problem obtained on its basis may be too complicated for modern algorithms for solving problems of this class [1].

The second type of computer network modeling is simulation modeling. This type of simulation is often the best, and sometimes the only way to study real systems, including networks.

The term "simulation modeling" means that the processes under study are difficult to predict, and to predict the behavior of a system, a computational experiment (imitation) is required with given initial data.

The difference between the analytical and simulation models is that in the latter, instead of an explicit mathematical description of the relationship between the input and output variables, the real system is divided into a number of fairly small (in functional terms) elements or modules [1]. Then, the behavior of the source system is simulated as the behavior of a set of these elements, which are connected in a certain way (by establishing the corresponding relationships between them) into a single whole. The computational implementation of such a model begins with the input element, then goes through all the elements until the output element of the model is reached.

2. MODELING

Now the most common approach in information systems design is to use expert estimates. According to this approach, experts in the field of computing tools, active network equipment, cable networks, design computing system to solve the specific task or class of tasks, based on their experience and expert estimates. This approach minimizes the cost of the design stage, quickly estimate the cost of implementing the information system. However, decisions obtained by using expert estimates are subjective, hardware and software requirements as the assessment of guarantees for efficiency of proposed system project are subjective too.

As an alternative may be used approach, which involves the development of models and modeling (simulation work - simulation) of computing system behavior. The modeling is a fundamental method for studying the behavior of complex systems [2-5].

The modeling is one of the main methods of knowledge, and a form of reflection of reality. The

modeling is to clarify or reproduction of certain properties of real objects, things and events through other objects, processes, events, or through abstract descriptions such as image, plan, map, set of equations, algorithms and applications.

The model is defined as "a system that is provided or material implemented, that is replaced the real object (system) in the process of cognition or analyzing, while retaining some of the most important features for its research, and its study gives us new information about the object.

Here are the main types of models used in practice to describe the different processes and systems:

- the conceptual model – the model describes the system using special characters, symbols, operations or using natural or artificial languages;
- the physical model - the system reproduces based on the ratio of similarity, that is resulting from the similarity of physical phenomena;
- the structural and functional model - as a model uses scheme (block diagram), tables, graphs, diagrams and drawings with special rules of their union and transformation;
- the math model is a math representation of reality, the description of some phenomenon or system using math concepts and symbols;
- the simulation model - economic and math model uses in the experimental study of system or phenomena by using personal computers.

These types of models can be used both individually and a few at a time, also, when you use simulation modeling, it involves all of these types or their separate techniques. The simulation model allows us to visualize the final or intermediate result dynamically, that is an important aspect for a successful understanding the received results by persons who did not participate in its development.

3. SIMULATION MODEL

Common definitions of term “simulation modeling”:

- it is the method allows to build models that describe the processes as they would take place in reality. Such model can be "played" for a single test or set of tests. The results will be determined by the random behavior of the process;
- it is the research method in which studied system is replaced by a model that accuracy describes the real system, with which experiments are conducted to obtain information about this system;
- it is the special case of math modeling. There is a class of objects, for which have not developed analytical models or solution methods of resulting model for various reasons. In this case, the analytical model is by the simulator or simulation model;
- it is logical and mathematical description of an object that can be used to experiment on your computer in order to design, analysis and assessment of the object.

Simulation modeling is used to study the behavior of the system by using math tools and computing equipment. The calculation of the required results may be automated by using computing technology, with only initial data, for example, been obtained statistically. It is especially important, when complex system that consist of many components is being used, because for calculation of required results you need to use cumbersome formulas usually. Simulation modeling is applied to study the behavior of various systems, including the information one [6-8].

Mainly in information systems modeling there is an aim to achieve information about request processing time or resource load level. As for computing networks, their simulation models reproduce the processes of message generation by applications, of splitting messages into specific protocols packets and frames, of delays in processing messages, packets and frames within the operating system, of computer access to the shared network environment, of router incoming packets processing and etc. No need to buy expensive equipment by using simulation modeling network - its work simulates by programs that accurately reproduce such equipment main features and options.

4. SIMULATION ENVIRONMENT

It was offered to use simulation modeling for determination the actual security threats [9-12]. GNS3 Cisco Systems software have been selected as the simulation environment (Fig 1).

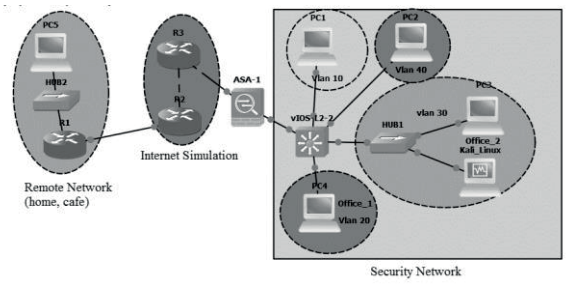


Fig.1 - The simulation model of information security system in computer network

The choice of this software due to the following factors:

- a process of creating models is facilitated by using a graphical development environment;

- previously created modules and libraries can be used to create new models;
- object-oriented approach to model building;
- a large number of built-in libraries for creating simulation models;
- models can be run at any software and hardware platform;
- a simulation model can be run without development tools.

Graphical Network Simulator GNS3 is a cross-platform program with open source. It is based on popular Dynamips (CISCO IOS emulator), Dynagen (Dynamips text interface) and Pemu (Cisco PIX emulator).

GNS3 provides easy to use GUI, and a range of other features. You can model the new configuration, various images of IOS, or perhaps, make fully reconstruction of some complex network parts. That is much easier with this program than its be in a real network. The product processes the installation and configuration of essential utilities automatically. The GNS3 installation package includes all emulators. In the case of GNS3 installation on the Microsoft Windows operating system, you must also install WireShark, it is necessary to intercept monitor network packets and libraries.

Sometimes, it is not enough network devices in the company and there is no router, which deals with internal networks routing, but there is only L2-switch and security device Cisco ASA with IOS 8.4.2 version. So, it is necessary to set additional functionality on Cisco ASA, such as routing. Similarly, we have only one interface to connect with the L2-switch. Also, we need to configure remote users' connections by VPN.

There is the next task: the networking between internal networks should be organize to meet the requirements of security. The guest network access should be organized only to "INTERNET" with limited speed of 1024 Kb. The remote users connect should be organize through Remote Access VPN, therefore remote users should connect to the internet via Cisco ASA device and have access to the internal resources of the company. Internal website should be available on "INTERNET". All of this task should be done through CLI. We have a central office with installed Cisco ASA device and L2-switch. Four networks (VLANs) have been created at switch, which submitted to security device through Trunk.

There are the characteristics of each VLAN-s:

- Vlan_Office_1 - network 192.168.2.0/24.

Security Level is 100. It is uses for first part of employees. There are the Internet access from this subnet, and Vlan_Office_2, Vlan_DMZ and Vlan_Guests access;

- Vlan_Office_2 - network 192.168.3.0/24.

Security Level is 100. It is uses for second part of employees. There are the Internet access from this subnet, and Vlan_Office_1, Vlan_DMZ and Vlan_Guests access;

- Vlan_DMZ - network 192.168.1.0/24.

Security Level is 50. There is a Web-Server (WWW-SRV) with company's website in this network. Accordingly, it is available from Internet at port 80 (TCP) and there are access from Vlan_Office_1, Vlan_Office_2 subnets to this network and from Vlan_Guests subnet at 80th port;

- Vlan_Guests - Guest subnet 192.168.4.0/24.

It is uses for "guests" who came to our office. Security Level is 10. There are the Internet access from this subnet with limit speed of 512 Kb and access to the internal website (SRV-WWW) only at 80th port.

There is a network, that simulates "INTERNET", which uses two routers (Router_1 and Router_2). There is loopback-interface (IP-address 1.1.1.1) at Router_1, which will be use to check for the "INTERNET". Dynamic routing protocol OSPF is used for routes exchange. Also, there is a remote user, which is placed in the subnet 192.168.5.0/24 (say it is internet-cafe) behind Remote_Router. This remote user has access to the Internet but he is considered dangerous without VPN connection to the central office.

A simulation model consists of protected and unprotected networks. The main element of information security system is the firewall ASA 8.4, a platform for attack- set Kali Linux. Kali Linux is modern Linux-distribution for penetration testing and security audit. Kali is a complete reassembly BackTrack Linux, fully according to Debian development standards.

All new infrastructure has been revised, all the tools were analyzed and packaged, and we switched to Git for our VCS.

- There are more than 300 tools for penetration testing: After considering each tool that was included in BackTrack, we have removed a large number of tools that either do not work or duplicate other tools with similar functionality.
- Kali Linux is completely free and always will be free. You will never have to pay for Kali Linux.
- Git tree with open source code: our tree is open to all, and all of sources available for set up or rebuild packages.
- FHS compliant: Kali was designed to observe the Filesystem Hierarchy Standard, which allows all Linux users easily find executable files, support files, libraries, etc.
- Wide support for wireless devices: Kali Linux was built to support many wireless devices, allowing

it to work correctly with a wide range of hardware devices and making it compatible with many USB and other wireless devices.

- Special core patches from injection: developers often need to audit wireless networks, so our core includes the latest patches for them.
- Secure Development Environment: Kali Linux development team consists of a small group of trusted persons who can add packages or interact with storage only by using several secure protocols.
- GPG signed packages and repositories: All packages are signed by each individual Kali developer when they are created and recorded, and then the repository signed packages also.
- Multilingual: Kali has a true multi-language support, allowing most users to work in their native language and to find the tools needed for the job.
- Customizable: You can as easy as possible customize Kali Linux to your taste, down to the core.
- Support ARMEL and ARMHF: Kali supports ARM-systems and has installations for ARMEL and ARMHF systems. Kali Linux ARM repository is integrated with the main distribution.

LOIC was used to implement attacks. The program performs a distributed attack such as "denial of service" by TCP-, UDP-packets or HTTP-requests regular transfer to the certain site or host with a goal to destroy the target node. There is also an edition of the program LOIC Hive Mind, that automatically receive the task to attack via IRC, RSS or Twitter, which allows centralized DDoS-attacks.

Attacks occur from a remote location to internal subnet (Office_1, Office_2, DMZ, Guests) with different security levels. There are customized security levels: offices - security level is 100, the traffic between offices is not filtered. DMZ security level – 50, Guests -10. Offices trafik is unrestricted with other subnets, there is access from DMZ to Guest subnet, there is access from the guest subnet only to the Internet. Internetworking is emulated by two routers with loopback-interface.

5. CONCLUSIONS

Using modeling in the design of computing systems, you can:

- estimate the bandwidth of the network and its components;
- identify vulnerability in the structure of computing system;
- compare different organizations of a computing system;
- make a perspective development forecast for computer system;
- predict future requirements for network bandwidth;
- estimate the performance and the required number of servers in the network;
- compare various options for computing system upgrading;
- estimate the impact of software upgrades, workstations or servers' power, network protocols changes on the computing system.

Research computing system parameters with different characteristics of the individual components allows us to select the network and computing equipment, taking into account its performance, quality of service, reliability and cost. As the cost of a single port in active network equipment can vary depends on the manufacturer's equipment, technology used, reliability, manageability.

The modeling can minimize the cost of equipment for the computing system. The modeling becomes effective when the number of workstations is 50-100, and when it more than 300, the total savings could reach 30-40% of project cost.

6. REFERENCES

[1] Klaus Wehrle, James Gross. *Modeling and Tools for Network Simulation*. Hardcover, 2010, 256 p.

[2] Korniyenko, B., Yudin, O. Galata, L. Research of the Simulation Polygon for the Protection of Critical Information Resources. *CEUR Workshop Proceedings, Information Technologies and Security, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017)*, Kyiv, Ukraine, November 30, 2017, Vol-2067, 2017, pp.23-31.

[3] Korniyenko, B. Model of Open Systems Interconnection terms of information security. *Science intensive technology*, № 3 (15), 2012, pp. 83 – 89.

[4] Korniyenko, B., Yudin, O., Novizki,j E. Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal*, issue 8, 2013, pp. 53 – 56.

[5] Korniyenko, B., Yudin, O. Implementation of information security a model of open systems interconnection. *Abstracts of the VI International Scientific Conference "Computer systems and network technologies»* (CSNT-2013), 2013, p. 73.

[6] Korniyenko, B. *Information security and computer network technologies*: *monograph*. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland, 2016, 102 p.

[7] Korniyenko, B., Galata, L., Kozuberda, O. Modeling of security and risk assessment in information and communication system. *Sciences of Europe*, V. 2., No 2 (2), 2016, pp. 61 -63.
[8] Korniyenko, B. The classification of information technologies and control systems. *International scientific journal,* № 2, 2016, pp. 78 - 81.
[9] Korniyenko, B., Yudin, O. Galata, L. Risk estimation of information system. *Wschodnioeuropejskie Czasopismo Naukowe*, № 5, 2016, pp. 35 - 40.
[10] Korniyenko, B., Galata, L., Udowenko, B. Simulation of information security of computer networks. *Intellectual decision-making systems and computing intelligence problems (ISDMCI'2016): Collection of scientific papers of the international scientific conference*, Kherson, Ukraine, 2016, pp. 77 - 79.
[11] Korniyenko, B. *Cyber security - operating systems and protocols*. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland, 2017, 122 p.
[12] Korniyenko, B., Galata, L. Design and research of mathematical model for information security system in computer network. *Science intensive technology*, № 2 (34), 2017, pp. 114 - 118.

Korniyenko Bogdan Yaroslavovich,
Education and qualifications: Doctor of Technical Sciences, Associate Professor
Employment: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Professor of the Department of Automation and Control in Technical Systems, since 2018.
Interests: information security, information technology
Science: Author of more than 160 scientific papers.

***Galata Liliya Pavlivna**,*
Education and qualifications:
- National Aviation University, engineer of computer systems, 2005;
- National Aviation University, the postgraduate study program for Doctors of Philosophy at the specialty 122 «Computer Science and Information Technologies», from 2017.
Employment: National Aviation University, assistant of the Department of computerized information security systems, since 2005.
Interests: information security, information technology, web development.
Science: author of more than 40 scientific publications.

DOI: https://doi.org/10.17721/ISTS.2019.1.42-51
УДК 004.056

ДО КОНЦЕПЦІЇ ЗАХИЩЕНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ

Бичков Олексій
orcid.org/0000-0002-9378-9535

м. Київ, Київський національний університет імені Тараса Шевченко, bos.knu@gmail.com

Історія статті:
Надійшла до редакції 02.10.2019
Прийнято 11.10.2019

Ключові слова:
захищеність;
операційна система;
вбудовані системи;
мікроконтролери;
інтернет речей

***Анотація**: На сучасному етапі використання інформаційних технологій у суспільстві, важливим стає питання захисту інформації. Основну роль в цьому відіграють операційні системи. На них покладається роль захисників усіх даних користувача та прав доступу до інформації.*

Перед авторами статті ставилась задача запропонувати класифікацію використання операційних систем та надати вимоги до механізмів захисту інформації за цією класифікацією. В статті автором:

- проаналізовано існуючі стандарти забезпечення безпеки, які реалізовано у сучасних операційних системах. Наведено існуючі стандарти забезпечення безпеки (Критерії оцінки комп'ютерних систем "Помаранчева книга», міжнародний стандарт – ISO 17799). У "Помаранчевій книзі" довірена система визначається як "система, що використовує достатні апаратні і програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу". Також розглянуто механізми безпеки і класи безпеки сучасних операційних систем і модель управління безпекою BS 7799. Цей стандарт містить систематичний, повний, універсальний перелік регулювальників безпеки, корисний для організації практично будь-якого розміру, структури і сфери діяльності системи управління інформаційною безпекою. В стандарті під системою управління інформаційною безпекою (СУІБ) (Information Security Management System, ISMS) розуміється частка загальної системи управління, що базується на аналізі ризику і призначена для проектування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси;

- проведено аналіз механізмів комплексної системи захисту інформації (КСЗІ) та забезпечення безпеки, які реалізовані в сучасних операційних системах;

- запропоновано класифікацію варіантів використання операційних систем у інформаційно-телекомунікаційних системах. Визначено вимоги до механізмів захисту інформації для операційних систем за класифікацією, що запропонована;

- запропоновано вимоги до стандарту захисту інформації операційної системи та вимоги до механізмів захищеності ОС в рамках класу використання.

***Abstract**: At the present stage of the use of information technologies in society, the issue of information protection becomes important. Operating systems play a major role in this. They are assigned the role of protectors of all user data and access rights.*

The authors of the article were tasked with proposing a classification of the use of operating systems and with the requirements for mechanisms of protection of information under this classification. In the article:

- the existing security standards that are implemented in modern operating systems are analyzed. Existing security standards are outlined (Trusted Computer System Evaluation Criteria «Orange Book», TCSEC, ISO 17799). In the Orange Book, a trusted system is defined as "a system that uses sufficient hardware and software to provide simultaneous processing of information of varying secrecy by a group of users without violating access rights." Security mechanisms and security classes of modern operating systems and BS 7799 security management model are also considered;

of safety regulators, useful for the organization of almost any size, structure and scope information security management system. The standard Information Security Management System (ISMS) refers to the proportion of the overall risk-based management system designed to design, implement, control, maintain and improve information security activities. This system consists of organizational structures, policies, planning actions, responsibilities, procedures, processes and resources;

- the analysis of the mechanisms of the complex system of information security (CSIS) and security, which are implemented in modern operating systems;

- classification of operating system usage variants in information and telecommunication systems is offered. Requirements for information security mechanisms for operating systems according to the proposed classification are defined;

- requirements for operating system information security standard and requirements for OS security mechanisms within the usage class are proposed.

this standard contains a systematic, complete, universal list

1. ВСТУП

Кількість атак на сервери і системи, що як локальні, без підключення, так і такі, що знаходяться в локальній мережі або в мережі Інтернет росте з кожним роком. Тому необхідно розробити правила, за допомогою яких ми визначатимемо, - наскільки можна назвати операційну систему захищеною, а також розробити стандартні правила, на основі яких кваліфікуватимемо встановлюване або таке, що розробляється ПО як захищене, або як таке, що порушує безпеку операційної системи [1-4].

1.1 Існуючі стандарти забезпечення безпеки. Проведення аналізу механізмів забезпечення безпеки, які реалізовано у сучасних операційних системах.

Критерії оцінки довірених комп'ютерних систем було запропоновано в “Помаранчевій книзі» [5], яка згодом стала міжнародним стандартом – ISO 17799.

Історично першим стандартом, що здобув широке розповсюдження і такий, що зробив величезний вплив на базу стандартизації в багатьох країнах, став стандарт Міністерства оборони США "Критерії оцінки довірених комп'ютерних систем". Він був вперше опублікований в серпні 1983 року. Мова йде не про безпечні, а про довірені системи, тобто системи, яким можна надати певний ступінь довіри. Дану працю називають найчастіше за кольором обкладинки "Помаранчевою книгою. "Помаранчева книга" пояснює поняття безпечної системи, яка "управляє, за допомогою відповідних засобів, доступом до інформації, так що тільки належним чином авторизовані особи або процеси, що діють від їх імені, отримують право читати, записувати, створювати і видаляти інформацію". Очевидно, проте, що абсолютно безпечних систем не існує, це абстракція. Є сенс оцінювати лише ступінь довіри, яку можна надати тій або іншій системі. У "Помаранчевій книзі" довірена система визначається як "система, що використовує достатні апаратні і програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу".

Британський стандарт BS 7799 [6] фактично теж має статус міжнародного (ISO/IEC 17799).

Перша частина стандарту, "Управління інформаційною безпекою. Практичні правила", містить систематичний, вельми повний, універсальний перелік регулювальників безпеки, корисний для організації практично будь-якого розміру, структури і сфери діяльності.

Ця частина призначена для використання як довідковий документ керівниками і рядовими співробітниками, що відповідають за планування, реалізацію і підтримку внутрішньої системи інформаційної безпеки.

Згідно стандарту, мета інформаційної безпеки - забезпечити безперебійну роботу організації, по можливості запобігти і/або мінімізувати збиток від порушень безпеки.

Управління інформаційною безпекою дозволяє колективно використовувати дані, одночасно забезпечуючи їх захист і захист обчислювальних ресурсів.

Підкреслюється, що захисні заходи виявляються значно дешевшими і ефективнішими, якщо вони закладені в інформаційні системи і сервіси на стадіях завдання вимог і проектування.

У стандарті виділяється десять ключових регулювальників, які або є обов'язковими відповідно до чинного законодавства, або вважаються за основні структурні елементи інформаційної безпеки.

У другій частині стандарту BS 7799-2:2002 "Системи управління інформаційною безпекою -

специфікація з керівництвом по використанню" предметом розгляду, як випливає з назви, є система управління інформаційною безпекою.

Також слід звернути увагу на захищеність операційних систем для мобільних приладів та вбудованих систем [7,8].

2. АНАЛІЗ СУЧАСНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 КЛАСИ БЕЗПЕКИ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ І МОДЕЛЬ УПРАВЛІННЯ БЕЗПЕКОЮ BS 7799

Проведений аналіз стандартів показав, що "Критерії ..." Міністерства оборони США відкрили шлях до ранжування інформаційних систем по ступеню довіри безпеки.

У "Помаранчевій книзі" визначається чотири рівні довіри - D, C, B і A. Рівень D призначений для систем, визнаних незадовільними. У міру переходу від рівня C до A до систем пред'являються все більш жорсткі вимоги. Рівні C і B підрозділяються на класи (C1, C2, B1, B2, B3) з поступовим зростанням ступеня довіри.

Всього є шість класів безпеки - C1, C2, B1, B2, B3, A1. Щоб в результаті процедури сертифікації систему можна було віднести до деякого класу, її політика безпеки і рівень гарантованості повинні задовольняти заданим вимогам, з яких ми згадаємо лише найважливіші.

Клас C1:

- довірена обчислювальна база повинна управляти доступом іменованих користувачів до іменованих об'єктів;

- користувачі повинні ідентифікувати себе, перш ніж виконувати які-небудь інші дії, контрольовані довіреною обчислювальною базою. Для аутентифікації повинен використовуватися який-небудь захисний механізм, наприклад пароль. Аутентифікаційна інформація має бути захищена від несанкціонованого доступу;

- довірена обчислювальна база повинна підтримувати область для власного виконання, захищену від зовнішніх дій (зокрема, від зміни команд і/або даних) і від спроб стеження за ходом роботи;

- захисні механізми мають бути протестовані на предмет відповідності їх поведінки системної документації.

Клас C2 (на додаток до C1):

- права доступу повинні гранулюватися з точністю до користувача. Всі об'єкти повинні піддаватися контролю доступу;

- при виділенні об'єкту, що зберігається, з пулу ресурсів довіреної обчислювальної бази необхідно ліквідовувати всі сліди його використання;

- кожен користувач системи повинен унікальним чином ідентифікуватися.

Клас B1 (на додаток до C2):

- довірена обчислювальна база повинна управляти мітками безпеки асоційованими з кожним суб'єктом і об'єктом, що зберігається;

- довірена обчислювальна база повинна забезпечити реалізацію примусового управління доступом всіх суб'єктів до всіх об'єктів, що зберігаються;

- група фахівців, що повністю розуміють реалізацію довіреної обчислювальної бази, повинна піддати опис архітектури, початкових і об'єктних кодів ретельному аналізу і тестуванню;

Клас B2 (на додаток до B1):

- забезпечуватися мітками повинні всі ресурси системи (наприклад, ПЗП), прямо або побічно доступні суб'єктам;

- до довіреної обчислювальної бази повинен підтримуватися довірений комунікаційний шлях для користувача, що виконує операції початковій ідентифікації і аутентифікації;

- має бути передбачена можливість реєстрації подій, пов'язаних з організацією таємних каналів обміну з пам'яттю;

- має бути продемонстрована відносна стійкість довіреної обчислювальної бази до спроб проникнення;

- модель політики безпеки має бути формальною. Для довіреної обчислювальної бази повинні існувати описові специфікації верхнього рівня, точно і що повно визначають її інтерфейс;

Клас B3 (на додаток до B2):

- для довільного управління доступом повинні обов'язково використовуватися списки управління доступом з вказівкою дозволених режимів;

- має бути передбачена можливість реєстрації появи або накопичення подій, що несуть загрозу політиці безпеки системи. Адміністратор безпеки має негайно сповіщатися про спроби порушення політики безпеки, а система, в разі продовження спроб має присікати їх найменш хворобливим способом;

- процедура аналізу має бути виконана для тимчасових таємних каналів;

- має бути специфікована роль адміністратора безпеки. Здобути права адміністратора безпеки можна тільки після виконання явних протокольованих дій;

- має бути продемонстрована стійкість довіреної обчислювальної бази до спроб проникнення.

Клас A1 (на додаток до B3):

- тестування повинне продемонструвати, що реалізація довіреної обчислювальної бази відповідає формальним специфікаціям верхнього рівня;

- окрім описових, мають бути представлені формальні специфікації верхнього рівня. Необхідно використовувати сучасні методи формальної специфікації і верифікації систем;

- механізм конфігураційного управління повинен розповсюджуватися на весь життєвий цикл і всі компоненти системи, що мають відношення до забезпечення безпеки;

- має бути описана відповідність між формальними специфікаціями верхнього рівня і початковими текстами.

Коротко класифікацію, що введена в "Помаранчевій книзі" можна сформулювати так:

рівень С - довільне управління доступом;

рівень В - примусове управління доступом;

рівень А – безпека, що верифікується.

З недоліків даної концепції варто відзначити, наприклад, повне ігнорування проблем, що виникають в розподілених системах.

У стандарті BS 7799-2:2002 застосована чотирьох фазна модель процесу управління інформаційною безпекою: планування – реалізація – оцінка – коректування (ПРОК).

Процес управління має циклічний характер; на фазі первинного планування здійснюється вхід в цикл. Як перший крок має бути визначена і документована політика безпеки організації.

Потім визначається зона дії системи управління інформаційною безпекою. Вона може охоплювати всю організацію або її частки. Слід специфікувати залежності, інтерфейси і припущення, пов'язані з межею між СУІБ і її оточенням; це особливо важливо, якщо в зону дії потрапляє лише частка організації. Велику область доцільно поділити на підобласті управління.

Ключовим елементом фази планування є аналіз ризику.

Результат аналізу ризику - вибір регулювальників безпеки. План повинен включати графік і пріоритети, детальний робочий план і розподіл обов'язків по реалізації цих регулювальників.

В стандарті наголошується, що систему управління інформаційною безпекою треба постійно удосконалювати, щоб вона залишалася ефективною . Цю мету переслідує четверта фаза розглядуваного в стандарті циклу - коректування. Вона може зажадати як щодо незначних дій, так і повернення до фаз планування (наприклад, якщо з'явилися нові погрози) або реалізації (якщо слід здійснити намічене раніше).

Завдання фази оцінки - виявити проблеми. На фазі коректування необхідно докопатися до їх коріння і усунути першопричини невідповідностей, щоб уникнути повторної появи. З цією метою можуть робитися як реактивні, так і превентивні дії, розраховані на середньострокову або довгострокову перспективу.

2.2. АНАЛІЗ МЕХАНІЗМІВ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ (КСЗІ) ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ, ЯКІ РЕАЛІЗОВАНІ В СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ.

Завдання ідентифікації і аутентифікації користувачів є ключовим завданням захисту інформації від несанкціонованого доступу, вирішуваною системою захисту інформації в будь-якій операційній системі, оскільки розмежувальна політика доступу до ресурсів формується за допомогою завдання прав доступу для користувачів операційної системи.

1. Дискреційний механізм управління доступом користувачів до файлових об'єктів.

Проаналізуємо вимоги до механізму.

КСЗІ повинна контролювати доступ суб'єктів (користувачів), що найменовують, до об'єктів, що найменовують (файлам, програмам, томам і так далі).

Для кожної пари (суб'єкт - об'єкт) має бути задане явне і недвозначне перерахування допустимих типів доступу (читати, писати і так далі), тобто тих типів доступу, які є санкціонованими для даного суб'єкта (індивіда або групи індивідів) до даного ресурсу (об'єкту).

КСЗІ повинна містити механізм, що запроваджує в життя дискреційні правила розмежування доступу.

Контроль доступу має бути застосовний до кожного об'єкту і кожного суб'єкта (індивідові або групі рівноправних індивідів).

Механізм, що реалізовує дискреційний принцип контролю доступу, повинен передбачати можливості санкціонованої зміни правил розмежування доступу (ПРД), зокрема, можливість санкціонованої зміни списку користувачів і списку об'єктів, що захищаються.

Право змінювати ПРД повинне надаватися виділеним суб'єктам (адміністрації, службі безпеці і так далі).

Наведемо реалізацію вимог:

У систему в ланцюжок обробки запитів на доступ до файлової системи встановлюється драйвер системи захисту, який здійснює контроль доступу користувачів до об'єктів згідно заздалегідь визначеним правилам.

Кожен користувач визначається такими параметрами: реальний ідентифікатор користувача (RUID), ефективний ідентифікатор користувача (EUID). Це дозволяє розмежовувати доступ до об'єктів для користувача (групи користувачів), здійснюючи при цьому контроль коректності запозичення прав, що принципово підвищує рівень захищеності системи.

Право змінювати ПРД надається виділеним суб'єктам (адміністрації, службі безпеці і так далі). Це забезпечується власне реалізацією механізму розмежування прав доступу, права на завдання (зміна) ПРД надаються тільки привілейованому користувачеві - адміністраторові безпеки з інтерфейсу КСЗІ.

2. Дискреційний механізм управління доступом користувачів до пристроїв.

Проаналізуємо вимоги до механізму.

Ті ж, що і для управління доступом до файлових об'єктів.

Наведемо реалізацію вимог.

Звернення до пристроїв в ОС Unix реалізується через файлову систему, при цьому як об'єкт виступають файли пристроїв, які можуть бути блокові (дискові пристрої - дисковод, CD-ROM і так далі), або символьні (клавіатура, миша і так далі). Драйвером КСЗІ здійснюється розмежування доступу до файлів пристрою (пристроям) для користувачів.

3. Дискреційний механізм управління доступом до видалених робочих станцій і серверів ЛВС по протоколу TCP(UDP) /IP.

Проаналізуємо вимоги до механізму.

Ті ж, що і для управління доступом до файлових об'єктів.

Наведемо реалізацію механізму.

До складу КСЗІ входить драйвер контролю доступу до мережевих ресурсів. Як об'єкти доступу виступають IP-адреса і значення портів доступу. Драйвер КСЗІ здійснює фільтрацію повідомлень дозволяючи взаємодіяти робочій станції в складі ЛВС тільки з комп'ютерами, що мають задані IP, - адреси, причому взаємодіяти тільки по заданих номерах портів.

4. Механізм очищення зовнішньої пам'яті.

Проаналізуємо вимоги до механізму.

При первинному призначенні або при перерозподілі зовнішньої пам'яті КСЗІ повинен запобігати доступу суб'єктові до залишкової інформації.

Наведемо реалізацію механізму.

Перерозподіл зовнішньої пам'яті можливий тільки в разі звільнення частки пам'яті, раніше займаної файлом. Це звільнення відбувається у момент видалення (або модифікації) файлу. Для запобігання доступу до залишкової інформації в КСЗІ використовується прикладна програма очищення зовнішньої пам'яті, яка перед видаленням (модифікацією) файлу автоматично затирає його (записує в нього нульові дані, або "всі одиниці" - кількість циклів перезапису "нулями і "одиницями" задається при налаштуванні КСЗІ), затираючи цим його початкову інформацію.

5. Механізм ідентифікації і аутентифікації.

Проаналізуємо вимоги до механізму.

КСЗІ повинна вимагати від користувачів ідентифікувати себе при запитах на доступ. КСЗІ повинна піддавати перевірці достовірність ідентифікації - здійснювати аутентифікацію. КСЗІ повинна мати в своєму розпорядженні необхідні дані для ідентифікації і аутентифікації. КСЗІ повинна перешкоджати доступу до ресурсів неідентифікованих користувачів і користувачів, що захищаються, достовірність ідентифікації яких при аутентифікації не підтвердилася.

Наведемо реалізацію механізму.

- заміна стандартної програми ОС аутентифікації користувачів (у ОС Linux вся ідентифікація і аутентифікація користувачів проводиться за допомогою такої програми) - login - на програму, що входить до складу КСЗІ, а також заміна стандартної програми ОС призначення паролів (завдання обмежень на пароль) користувачам passwd.

- ідентифікація і аутентифікація операторів при вході в ОС по ідентифікатору (коду) і паролю умовно-постійної дії;

- перевірка складності пароля (пароль повинен містити не менше двох букв і не менш однієї цифри, пароль не повинен повторювати імені користувача або бути якою-небудь модифікацією імені користувача) і терміну його дії;

- для кожного облікового запису передбачена можливість ведення історії паролів;

- блокування облікових записів операторів при введенні невірного пароля з розблокуванням через службу адміністратора безпеки.

6. Механізм реєстрації (аудиту) подій.

Проаналізуємо вимоги до механізму.

КСЗІ повинна здійснювати реєстрацію наступних подій:

- використання ідентифікаційного і аутентифікаційного механізму;

- запит на доступ до ресурсу, що захищається (відкриття файлу, запуск програми і так далі);

- створення і знищення об'єкту;

- дії із зміни ПРД.

Для кожної з цих подій повинна реєструватися наступна інформація:

- суб'єкт, що здійснює реєстровану дію;

- дата і час;

- тип події (якщо реєструється запит на доступ, то слід відзначати об'єкт і тип доступу);

- чи вдало здійснилася подія (обслужений запит на доступ чи ні).

КСЗІ повинна містити засоби вибіркового ознайомлення з реєстраційною інформацією.

Наведемо реалізацію механізму.

- реєстрація входу (виходу) операторів до ОС, або реєстрації завантаження і ініціалізації операційної системи і її програмного останову;

- реєстрація запуску/завершення програм і процесів;

- реєстрація спроб доступу користувачів і програмних засобів (програм процесів) до томів, що захищаються, каталогів і файлів;

- дії із зміни ПРД і так далі.

Кожен власний механізм захисту КСЗІ веде реєстрацію заданих адміністратором безпеки подій, реєструючи потрібні вище параметри.

7. Механізм контролю цілісності КСЗІ.

Проаналізуємо вимоги до механізму.

Мають бути передбачені засоби періодичного контролю цілісності програмної і інформаційної частки КСЗІ.

Наведемо реалізацію механізму.

Цілісність КСЗІ контролюється підсистемою контролю цілісності файлової системи. Вона реалізована у вигляді додаткової програми, яка через заданий інтервал часу перевіряє набір файлів, що задається адміністратором, на предмет зміни їх контрольної суми, розміру, часу останньої модифікації. При виявленні невідповідності (при завданні відповідній опції адміністратором) проводиться автоматичне відновлення файлів з резервної копії.

КСЗІ здійснює періодичний контроль цілісності не лише власних файлів, але і будь-яких інших файлів (по вибору адміністратором), які розташовані на робочій станції, що захищається, задаються для контролю адміністратором безпеки.

8. Дискреційний механізм управління доступом процесів до файлових об'єктів і до пристроїв.

Проаналізуємо вимоги до механізму.

КСЗІ повинна забезпечувати дискреційний доступ до об'єктів і пристроїв

Наведемо реалізацію механізму.

У ланцюжок обробки запитів на доступ до файлової системи і до пристроїв встановлюється драйвер системи захисту, який здійснює контроль доступу процесів до об'єктів згідно заздалегідь визначеним правилам.

Кожен суб'єкт доступу визначається не лише параметрами користувача: реальний ідентифікатор користувача (RUID), ефективний ідентифікатор користувача (EUID), але і параметром процесу - процес, що виконує дію. Це дозволяє розмежовувати доступ до об'єкту не лише для користувача (групи користувачів), але і для процесу. КСЗІ реалізує розмежування доступу, як тільки для користувача (доступ до об'єкту дозволений, якщо він дозволений користувачеві, що звертається до об'єкту) або тільки для процесу (доступ до об'єкту дозволений, якщо він дозволений процесу, що звертається до об'єкту), так для користувача і процесу разом (доступ до об'єкту дозволений, якщо він дозволений користувачеві і процесу одночасно).

КСЗІ надає адміністраторові вельми сильний механізм протидії погрозам, проте адміністратор повинен відповідним чином набудувати механізм з урахуванням особливостей прояву погроз, від яких слід захищати комп'ютер.

9. Забезпечення замкнутості програмного середовища.

Проаналізуємо вимоги до механізму.

Це найважливіший механізм захисту, який є основним механізмом протидії прихованим погрозам. Коректне його налаштування не дозволить зловмисникові запускати власні програми, як наслідок, позбавить його якого-небудь інструментарію протидії системі захисту. Крім того, даний механізм є одним з основних механізмів антивірусної протидії. Даний механізм захисту обов'язково має бути активізований і настроєний.

Наведемо реалізацію механізму.

Для кожного користувача можна встановити розмежування на запуск програм, тобто для кожного користувача можна задати список дозволених йому для запуску процесів. Дозволені для запуску програми задаються їх повнопутніми іменами (або каталогами, з яких можуть запускатися файли, або масками). При забороні модифікації відповідних файлів (засобами розмежування доступу до файлової системи), користувач не має можливості підмінити дозволені йому на запуск програми. Оскільки при запуску програми аналізується її повний шлях розташування у файловій системі, то користувач не має можливості запустити власний процес під ім'ям дозволеного до запуску.

Даний механізм реалізується власним драйвером. Перед запуском процесу, драйвер аналізує повнопутнє ім'я процесу, на предмет входження даного імені в список дозволених для запуску процесів для користувача. У випадку, якщо процесу з даним повнопутнім ім'ям в списку не існує, КСЗІ не дозволить здійснити його запуск.

10. Механізм контролю цілісності програм перед запуском.

Проаналізуємо вимоги до механізму.

У КСЗІ має бути присутнім механізм відстежування несанкціонованої модифікації системних файлів при їх використанні, а також наявність можливості періодичної перевірки і перевірка цілісності системних файлів при запуску операційної системи. При виявленні несанкціонованої модифікації системних файлів (при завданні відповідній опції адміністратором) повинно проводиться автоматичне відновлення файлів з резервної копії.

Наведемо реалізацію механізму.

Цілісність програм перед запуском контролюється підсистемою, виконаною у вигляді окремої прикладної програми. Адміністратором безпеки задаються програми, які повинні контролюватися перед запуском на предмет зміни їх контрольної суми, розміру, часу останньої модифікації. Перед запуском контрольованої програми драйвером КСЗІ передається управління даній прикладній програмі, що здійснює контроль. При виявленні невідповідності (при завданні відповідній опції адміністратором) проводиться автоматичне відновлення контрольованої програми з резервної копії, після чого вона запускається, або забороняється запуск модифікованої програми.

11. Механізм управління доступом до монтування пристроїв.

Проаналізумо вимоги до механізму.

Механізм повинен реалізовувати права доступу для кожного користувача по відношенню до кожного пристрою

Наведемо реалізацію механізму.

Для підключення до системи пристрою (дисковода, CD-ROM приводу і ін.) його необхідно змонтувати - "підключити" до файлової системи (до каталога). "Точкою" підключення пристрою до файлової системи визначається повнопутнє ім'я пристрою. КСЗІ дозволяє розмежовувати доступ до монтування пристроїв, за допомогою завдання до яких каталогів, які пристрої і з якою файловою системою можуть вмонтовуватися.

12. Механізм аутентифікації при завантаженні в режимі Single-User Mode.

Проаналізуємо вимоги до механізму.

Ідентифікація і аутентифікація перед запуском даного режиму, причому ця можливість має бути доступна тільки адміністраторові системи.

Наведемо реалізацію механізму.

У процес початкового завантаження системи вбудовується механізм (власними засобами КСЗІ змінена стартова процедура завантаження системи) що запобігає неаутентифікованому завантаженню системи в режимі Single-User Mode (цей аварійний режим дозволяє здійснити вибіркове завантаження системи, зокрема без драйверів КСЗІ). За умовчанням вхід в даний режим доступний будь-якому користувачеві системи. КСЗІ вимагає проведення ідентифікації і аутентифікації перед запуском даного режиму, при цьому "за умовчанням" дозволяє доступ до запуску режиму тільки адміністраторові (після його авторизації).

13. Механізм надання привілеїв адміністраторові безпеки.

Проаналізуємо вимоги до механізму.

Даний механізм призначений для підвищення прав адміністраторові безпеки в порівнянні з "root", що дозволяє функціонально розмежовувати завдання системного адміністратора, якому належать права "root" і адміністратора безпеки.

Наведемо реалізацію механізму.

Механізм забезпечує неможливість проводити які-небудь дії, щодо процесів КСЗІ користувачеві з правами "root". При цьому, оскільки КСЗІ розмежовує доступ до об'єктів, зокрема до налаштувань КСЗІ власними засобами, користувач з правами "root" не має можливості впливати на функціонування КСЗІ.

3. МЕТА СТАТТІ

Метою статті є висвітлення існуючих стандартів безпеки інформаційних систем і механізмів комплексної системи захисту інформації та запропонувати класифікацію варіантів використання операційних систем у інформаційно-телекомунікаційних системах.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Будемо вважати операційну систему захищеною, якщо вона забезпечує збереженість інформації та цілісність даних власними засобами без використання допоміжного програмного забезпечення.

Основною задачею захищеної операційної системи є запобігання несанкціонованому доступу до даних із зовнішніх (по відношенню до неї) джерел. Тому ми будемо класифікувати операційні системи, по особливостях алгоритмів управління ресурсами – локальні і мережеві ОС.

Локальні ОС управляють ресурсами окремого комп'ютера. Мережеві ОС беруть участь в управлінні ресурсами мережі.

4.1. КЛАСИФІКАЦІЯ ОПЕРАЦІЙНИХ СИСТЕМ ЗА ВАРІАНТАМИ ВИКОРИСТАННЯ

Наведемо таку класифікацію операційних систем за варіантами використання.

1. ОС для використання на робочій станції, не

підключеній до мережі передачі даних.

2. ОС для використання на робочій станції, підключеній до внутрішньої мережі інтранет.

3. ОС для використання на робочій станції, підключеній до зовнішньої мережі інтернет.

4. ОС для використання на серверах, підключених у внутрішній мережі інтранет.

5. ОС для використання на серверах, підключених в зовнішній мережі інтернет.

Ми називатимемо сторонніми компонентами операційної системи, компоненти, не використання яких не є критичним для нормального функціонування системи локально або в мережі передачі даних

Часткою системи ми називатимемо ті компоненти, які необхідні для безвідмовного захищеного функціонування системи локально і при підключенні мережі передачі даних, а також механізми захисту доступу до інформації і контролю цілісності.

Не часткою системи ми вважатимемо компоненти, які вносять корективи до системних налаштувань і у яких є функція отримання інформації із-за зовнішнього периметра захисту операційної системи.

Будемо вважати операційну систему такою, що задовольняє стандарту захищеної операційної системи України, якщо вона включає такі компоненти (механізми): пакетний фільтр, механізм розмежування доступу до інформації, механізми очищення; механізм реєстрації системних подій, механізм управління і розподілу пам'яті, механізм шифрування і криптоалгоритмів, механізм резервного копіювання, механізм захисту від збоїв, механізм підключення до мережі і управління налаштуваннями підключення, механізм трансляції мережевих адрес, механізм підключення додаткових пристроїв до системи і їх управління, механізм контролю цілісності системи, механізм захисту файлової системи, механізм відновлення системи, механізм управління системними сервісами і драйверами, механізм запуску завдань за розкладом;

4.2. ВИМОГИ ДО СТАНДАРТУ ЗАХИСТУ ІНФОРМАЦІЇ ОПЕРАЦІЙНОЇ СИСТЕМИ

Сформулюємо певні вимоги до захищеної операційної системи.

1. Пакетний фільтр має забезпечувати:

- можливість створення окремих правил для всіх мережевих інтерфейсів;

- можливість створення окремих правил управління доступом для вихідного і вхідного трафіку;

- можливість створення правила «Що явно не дозволене – заборонено»;

- правила, що допускають вільне безперешкодне переміщення внутрішніх пакетів на локальні інтерфейси і адресу 127.0.0.1;

- можливість заносити в лог пакети для кожного правила;

- правила, для яких частіше виконується відповідність, мають бути написані вище за правила, для яких відповідність виконується рідше. Останнє правило в розділі повинно блокувати і заносити в лог всі пакети даного інтерфейсу і напряму;

- не повинна відправлятися відповідь на небажані пакети, що блоковані засобами операційної системи, тобто щоб той, хто атакує не знав чи досягли його пакети мети;

- можливість створення динамічного правила для віддзеркалення атак типу «відмова у обслуговуванні». Мається на увазі обмеження кількості одночасно встановлюваних сесій за допомогою огляду полів джерела або одержувача в правилі, яке виконується, якщо встановлений ліміт одночасних сесій. Якщо значення лічильника більше чим значення, що вказане в ліміті, – пакет відкидається;

- можливість текстової фільтрації трафіку (відкидати або пропускати пакети, в яких зустрічаються символи або рядки, що задовольняють встановленим правилам).

2. Засоби розмежування доступу до інформації

- має бути задане явне і недвозначне перерахування допустимих типів доступу (читання, запис, виконання, виконання з більш вищими привілеями) для кожного суб'єкта або групи по відношенню до об'єкту (ресурсу);

- контроль доступу має бути застосовний до кожного об'єкту і кожному суб'єктові;

- можливість змінювати правила доступу повинно надаватися виділеним суб'єктам (адміністраторам, довіреним групам);

3. Механізми очищення

- повинне здійснюватися очищення тих, що звільняються областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів. Очищення здійснюється довільним записом в область пам'яті, що звільняється, раніше використану для зберігання даних, що захищаються (файлів);

- має здійснюватися очищення тимчасових системних файлів;

- архівація результатів моніторингу і відправка їх на сервер зберігання резервних копій, з подальшим видаленням незапакованих файлів з метою зменшити об'єм займаного місця;

4. Механізм реєстрації системних подій

- всі події в системі, які мають відношення до роботи системи безпосередньо, до безпеки і до

призначених для користувача застосувань винні фіксуватися і записуватися;

5. Критерій витривалості атаки: операційна система повинна встигнути записати повний моніторинг дій зловмисника

- підтримка стабільної роботи системного моніторингу на протязі моніторингу атаки з повною фіксацією дій зловмисника і паралельною відправкою на сервер резервних копій;

6. Вимоги до паролів

- механізм встановлення паролів не повинен допускати установки слабих паролів менше 8 символів і що мають осмислене значення;

7. Механізм розподіленої пам'яті для процесів, об’єктів ядра, файлових і мережевих дескрипторів

- процеси і об'єкти ядра не повинні мати можливості по власній ініціативі міняти дані інших процесів або об'єктів ядра.

8. Механізм шифрування і криптоалгоритмів

- у системі мають бути інтегрована можливість здійснювати криптографічний стійкий захист даних від несанкціонованого доступу;

- система повинна використовувати інтегроване шифрування файлової системи при якому неможливо зчитати дані при знятті накопичувача і підключення його до іншого комп'ютера;

9. Відомості про операційну систему і сервіси

- система не повинна давати інформацію про своє найменування, версію і версії працюючих сервісів неавторизованому користувачеві;

10. Механізм резервного копіювання даних

- у систему має бути вбудований механізм, що забезпечує передачу даних на видалений сервер резервного копіювання;

11. Механізм захисту від помилок переповнювання буфера

- наявність механізму, який би на рівні ядра забороняв виконання коду з адресного сегменту даних;

12. Механізм сповіщення про успішні і невдалі спроби авторизації

- механізм повинен в реальному часі повідомляти адміністратора або групу довірених осіб про вироблювані спроби авторизації або підвищення привілеїв у системі;

- всі спроби повинні записуватися у файл і передаватися на резервний сервер зберігання даних;

13. Механізм контролю доступу пристроїв, що підключаються

- наявність системних таблиць з описом прав доступу для підключення пристрої для кожного користувача зі встановленими дозволами використання (читання, запис, виконання);

14. Механізм управління процесами

- має бути реалізований механізм управління процесами в системі;

- кожен користувач може управляти процесами його групи, але не має доступу до більш вищих процесів;

15. Механізм підтримки цілісності системи

- наявність механізму відстежування несанкціонованої модифікації системних файлів при їх використанні, а також наявність можливості періодичної перевірки і перевірка цілісності системних файлів при запуску операційної системи;

- при виявленні несанкціонованої модифікації системних файлів (при завданні відповідній опції адміністратором) проводиться автоматичне відновлення файлів з резервної копії;

16. Механізм відновлення системи

- можливість відновлення системи після збою, пошкодження системні файлів, можливість створення контрольної точки відновлення;

17. Локальне блокування системи у відсутності користувача, що авторизувався

- можливість локально заблокувати доступ до системи на якийсь час відсутність користувача;

18. Механізм налагодження мережевих з'єднань

- можливість управляти налаштуванням підключення до мережі і параметрами підключення тільки адміністраторові або групі довірених осіб можливість управління правами доступу до мережі для різних користувачів;

19. Механізм управління системними сервісами

- управління системними сервісами і драйверами можливо тільки адміністраторові або групі довірених осіб;

20. Загальні критерії

- здобути права адміністратора безпеки можна тільки після виконання явних, протокольованих дій;

- вхід в систему під single-user повинен вимагати авторизації;

- користувачі повинні пройти ідентифікацію і аутентифікацію перш ніж виконувати які-небудь дії в системі

- аутентифікаційна інформація має бути захищена від несанкціонованого доступу;

- кожна реєстрована дія повинна асоціюватися з конкретним користувачем.

Зазначені вимоги мають скласти ядро захищеної операційної системи реального часу.

6. ВИСНОВОК

В статті проведено аналіз існуючих стандартів забезпечення безпеки, які реалізовано у сучасних операційних системах. Також проведено аналіз механізмів комплексної системи захисту інформації (КСЗІ) та забезпечення безпеки, які реалізовані в сучасних операційних системах.

Автором запропоновано класифікацію варіантів використання операційних систем у інформаційно-телекомунікаційних системах. На основі отриманих результатів пропонується в подальшому визначити вимоги до механізмів захисту інформації для операційних систем за класифікацією, що запропонована та запропонувати вимоги до стандарту захисту інформації операційної системи та вимоги до механізмів захищеності ОС в рамках класу використання.

7. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Multilevel Secure Operating Systems // Journal Of Information Science And Engineering 15, 91-106 (1999).

[2] Bell E., LaPaduIa L. Secure Computer Systems: A Mathematical Model // MITRE Technical Report 2547, Volume II, 1973.

[3] McLean J. Security models // Encyclopedia of software engineering, 1994

[4] Bell E., LaPaduIa L. Secure Computer Systems: Mathematical Foundations // MITRE Technical Report 2547, Volume I, 1973.

[5] Trusted Computer System Evaluation Criteria [Online]. Available: https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria

[6] Code of Practice for Information Security Management [Online]. Available: https://ru.wikipedia.org/wiki/BS_7799-1

[7] Фроимсон Л.И., Кутепов С.В., Тараканов О.В., Шереметов А.В. Основные принципы построения защищенной операционной системы для мобильных устройств. Спецтехника и связь. – 2013.- №1.-С.43-47

[8] SeLinux documentation. National security agency, 2011- [Online]. Available: http://www.nsa.gov/research//selinux/docs.html

***Бичков Олексій Сергійович**, доктор технічних наук, доцент, завідувач кафедри Програмних систем і технологій Київського національного університету імені Тараса Шевченка. Область наукових інтересів: математичні моделі систем захисту інформації, теорія гібридних автоматів, теорія можливості.*

DOI: https://doi.org/10.17721/ISTS.2019.1.52-56
УДК 629.391

КОДУВАННЯ БІТОВОГО ПРЕДСТАВЛЕННЯ ТРАНСФОРМАНТ У РАМКАХ УПРАВЛІННЯ БІТОВОЮ ШВИДКІСТЮ ВІДЕО

Бараннік Володимир [1]
orcid.org/0000-0002-2848-4524

Рябуха Юрій [2]
orcid.org/0000-0003-4235-300X

Гуржий Павло [3]
orcid.org/0000-0002-2996-9523

Твердохліб Віталій [4]
orcid.org/0000-0002-2552-229X

Шевченко Ігор [5]
orcid.org/0000-0003-4556-497X

[1] Харківський національний університет Повітряних сил імені Івана Кожедуба, Україна. Харків, вул. Сумська 77/79, vvbar.off@gmail.com
[2] Харківський національний університет Повітряних сил імені Івана Кожедуба, Україна. Харків, вул. Сумська 77/79, vvbar.off@gmail.com
[3] Військовий інститут телекомунікацій та інформатизації, Україна, Київ, pavel.nik.563@gmail.com
[4] Харківський національний університет радіоелектроніки, Україна. Харків, просп. Науки 14, vitalii.tverdokhlib@nure.ua
[5] Харківський національний університет радіоелектроніки, Україна. Харків, просп. Науки 14, igor96sheva@gmail.com

Історія статті:
Надійшла до редакції 21.06.2019
Прийнято 30.07.2019

Ключові слова:
бітова площина;
відеопоток;
трансформанта ДКП;
бітова швидкість

Анотація: *Розглядаються концептуальні засади побудови ефективного методу кодування у складі модулю управління бітовою швидкістю трафіку відео у системі обробки відеоданих на рівні джерела. Розкривається сутність використання запропонованого методу у ході управління бітовою швидкістю відео потоку, а саме – принципи побудови кодового представлення фрагмента кадру та підходи щодо визначення структурних одиниць окремого відеокадру, у рамках якого здійснюється управління. Метод орієнтується на обробку бітового представлення трансформант ДКП, при цьому, на даному етапі обробки трансформанта розглядається як структурна складова кадру відео потоку, на рівні якої здійснюється кодування. У той же час, для забезпечення гнучкості управління бітовою швидкістю відеотрафіку, відносно кожної з трансформант виконується декомпозиція до рівня множини бітових площин. Доводиться, що запропонований підхід потенційно здатний забезпечити зменшення бітової швидкості відеопотоку за найгірших умов, тобто, коли виконується компонентне кодування. Окрім того, такий принцип формування кодового представлення фрагменту відео потоку дозволяє контролювати рівень помилки, яку може бути внесено у процесі управління бітовою швидкістю. При цьому в умовах, коли здійснюється кодування бітового представлення трансформант, метод здатен забезпечити вищі показники стиснення як наслідок того, що значення ймовірності виявлення довжин двійкових серій та величини виявлених довжин у межах бітової площини будуть більшими, ніж у випадку компонентного кодування. Це пояснюється структурними особливостями розподілу двійкових елементів у межах кожної з бітових площин, які разом формують трансформанту ДКП. Зокрема, високочастотні області трансформант частіше за все формується ланцюжками нульових елементів. Рішення, запропоновані у рамках розробки методу кодування, здатні забезпечити достатню гнучкість управління бітовою швидкістю потоку відео, а також можливість оперативної зміни бітової швидкості у широкому діапазоні значень.*

Abstract: *The conceptual basements of constructing an effective encoding method within the bit rate control module of video traffic in the video data processing system at the source level are considered. The essence of using the proposed method in the course of the video stream bit rate controlling disclosed, namely, the principles of constructing the fragment of the frame code representation and approaches for determining the structural units of the individual video frame within which the control is performed. The method focuses on processing the bit representation of the DCT transformants, and at*

his processing stage transformant was considered as a structural component of the video stream frame at which the encoding is performed. At the same time, to ensure the video traffic bit rate controlling flexibility, decomposition is performed with respect to each of the transformants to the level of the plurality of bit planes. It is argued that the proposed approach is potentially capable to reducing the video stream bit rate in the worst conditions, that is, when component coding is performed. In addition, this principle of video stream fragmen code representation forming allows to control the level of error that can be made in the bit rate control process. However, in conditions where the bit representation of the transformant is encoded, the method is able to provide higher compression rates as a result of the fact that the values of the detection probability of binary series lengths and the values of detected lengths within the bit plane will be greater than in the case of component coding. This is explained by the structural features of the distribution of binary elements within each of the bit planes, which together form the transformer DCT. In particular, high-frequency transformer regions are most often formed by chains of zero elements. The solutions proposed in the development of the encoding method are able to provide sufficient flexibility to control the bit rate of the video stream, as well as the ability to quickly change the bit rate in a wide range of values.

1. ВСТУП

В умовах, коли об'єми трафіку, що передаються мережею, невпинно зростають, питання ефективної обробки даних є актуальними. При цьому, найбільш гострим є питання обробки відеоданих, позаяк між інших типів трафіку відео є найбільш вимогливим за показниками часу обробки, чутливості до втрати окремих фрагментів даних та потребує суттєвого рівня пропускної здатності мережі для здійснення ефективної передачі.

У рамках рішення задач, пов'язаних з обробкою відеотрафіку, традиційно використовувались підходи, що базувались на:

- обробці відеоданих на рівні джерела (застосування технологій кодування);
- обробці відеоданих на рівні мережевих вузлів (пріоритизація трафіку, обробка черг відповідно пріоритету та ін.).

Як перший, так і другий підходи у сьогоднішніх умовах є недостатньо ефективними [1,2] як наслідок того, що пульсуючий характер відеоданих, що надходять у мережу, та пропускна здатність, мають різну природу [3-5] та формуються різними та незалежними складниками.

У цих умовах ефективним є рішення, що ґрунтується на управлінні бітовою швидкістю відеоданих у процесі трансляції.

2. ОСНОВНА ЧАСТИНА

У загальному вигляді управління являє собою процес зміни кількості біт, задіяних для опису структурної одиниці відео потоку, відповідно до змін пропускної здатності мережі. При цьому від того, на рівні яких структурних одиниць відеопотоку буде здійснюватися управління, залежать такі його показники, як:

- оперативність зміни бітової швидкості;
- доступний діапазон зміни рівня бітової швидкості;
- забезпечена якість обробки [6-9, 13-15].

Отже, така структурна одиниця повинна описуватися достатньою кількістю біт, при чому повинна забезпечуватися можливість варіації величини зміни бітової швидкості у процесі управління.

За таких умов недоцільним є вибір групи кадрів або окремого кадру відеопотоку у якості такої структурної одиниці. Натомість пропонується управління бітовою швидкістю здійснювати у рамках однієї трансформанти кадру [10-12, 16, 17], або їх сукупності, сформованої у слайс. При цьому, додатковий механізм зміни діапазону бітової швидкості може бути забезпечено шляхом декомпозиції трансформанти до рівня окремих бітових площин. За рахунок цього може здійснюватися маніпулювання об'ємом даних, що надсилаються у мережу. У таких умовах актуальним є питання ефективного кодування відеопотоку на рівні обраних структурних одиниць – бітових площин. Це пояснюється тим, що у рамках стандартизованих технологій кодування трансформанта розглядається як єдиний об'єкт. Таким чином, метою статті є розробка методу кодування, що забезпечить гнучку обробку фрагментів відеопотоку. При цьому, окремі кодові описи таких фрагментів повинні бути незалежні один з іншими.

Пропонується метод позиційного кодування, який базується на використанні нерівновагових кодів для опису трансформанти. У цьому випадку, кодовий опис трансформанти може здійснюватися як на рівні компонент, так і на рівні сукупності бітових площин.

Розглянемо випадок, коли кодується компонентний опис трансформанти. Тоді будуть оброблятися ланюжки двійкових даних у напрямку зниження індексу розрядів компонент $\{\beta_{k\ell}^{(n)}, \beta_{k\ell}^{(n-1)},...,\beta_{k\ell}^{(1)}\}$, де $k=\overline{1,h}$, $\ell=\overline{1,w}$. У цьому випадку такі послідовності є двійковою формою опису компонент $c_{k\ell}$ у рамках трансформанти ДКП, як показано наступним виразом:

$$y(p)_{k\ell}=\beta_{k\ell}^{(n)}2^{n-1}+...+\beta_{k\ell}^{(n-\xi)}2^{n-\xi-1}+... \\ ...+\beta_{k\ell}^{(2)}2+\beta_{k\ell}^{(1)}, \quad (1)$$

де $\beta_{k\ell}^{(n-\mu)}$ являє собою $(n-\mu)$-й двійковий елемент компоненти з координатами $(k;\ell)$ у межах трансформанти, $(n-1)\geq\mu\geq 0$;

$2^{n-\mu-1}$ - ваговий коефіцієнт елементу $\beta_{k\ell}^{(n-\mu)}$ двійкового опису;

n - число розряів для опису компоненти.

Результатом виявлення довжин двійкових серій у напрямку розрядів компоненти є послідовність $\{\ell(1)_{k\ell}^{(q,i)},...,\ell(\theta)_{k\ell}^{(q,i)},...,\ell(\Theta)_{k\ell}^{(q,i)}\}$, у якій $\ell(\theta)_{k\ell}^{(q,i)}$ - довжина θ-ї двійкової серії, яку будо виявлено у межах двійкового опису $(k;\ell)$-ї компоненти q-ї трансформанти, що відноситься до i-го кадра. При цьому, серії починають виявлятись з елементу $y(n)_{k\ell}^{(q,i)}$. Нехай при цьому елементу $y(n)_{k\ell}^{(q,i)}$ передує серія нульових елементів, довжина якої буде 1. Тоді за умови, що $y(n)_{k\ell}^{(q,i)}=1$, відповідно $\ell(1)_{k\ell}^{(q,i)}=1$. Інакше спостерігається $\ell(1)_{k\ell}^{(q,i)}\geq 2$.

Очевидно, що буде мати місце скорочення надмірності, коли наступна нерівність буде справедливою, а саме:

$$E_{k\ell}<2^{n}, \quad (2)$$

де $E_{k\ell}$ - значення коду, який було побудовано для $(k;\ell)$-ї послідовності довжин.

Також при цьому припустимо, що все значення довжин двійкових серій рівні 1, $\ell_{k\ell}^{(\theta)}=1$, $\theta=\overline{1,\Theta}$. У цих умовах спостерігається кількість переходів γ_{bt} між двійковими послідовностями, яка буде рівна максимальному значенню $\gamma_{bt}=n$, тобто, кількість серій буде рівна кількості розрядів на опис компоненти $\Theta=n$. Тоді послідовність $\{\ell_{k\ell}^{(1)},...,\ell_{k\ell}^{(\theta)},...,\ell_{k\ell}^{(\Theta)}\}$ буде належати множині двійкових чисел, які будуть мати відображення $E_{k\ell}$ у вигляді позиційного числа за основою 2, тобто:

$$E_{k\ell}=\ell_{k\ell}^{(1)}2^{\Theta-1}+...+\ell_{k\ell}^{(\theta)}2^{\Theta-\theta}+... \\ ...+\ell_{k\ell}^{(\Theta-1)}2+\ell_{k\ell}^{(\Theta)}. \quad (3)$$

Оскільки при цьому для максимальної кількості двійкових переходів значення половини елементів $\beta_{k\ell}^{(\mu)}$ буде нульовим, справедливою буде нерівність $E_{k\ell}>y(p)_{k\ell}$.

У той же час, позаяк апріорі невідомо, що мінімальне значення довжини серії буде рівним 1, за рахунок зниження за замовчуванням динамічного діапазону довжин серій на 1 одержимо значення $E'_{k\ell}$, яке буде рівне 0, а саме:

$$E'_{k\ell}=(\ell_{k\ell}^{(1)}-1)2^{\Theta-1}+... \\ ...+(\ell_{k\ell}^{(\Theta-1)}-1)2+(\ell_{k\ell}^{(\Theta)}-1)=0. \quad (4)$$

Тоді буде справедливою нерівність $E'_{k\ell}<y(p)_{k\ell}$ Таким чином, вирар (2) також також буде справедливим та буде спостерігатися зниження кількості біт для опису компоненти.

Для збільшення довжин двійкових серій, прийнятнішим буде варіант обробки бітового опису трансформант у напрямку бітових площин. Тут використовується закономірність, згідно якій одиничні елементи у межах бітової площин старших порядків, що відносяться до високочастотних компонент, з великою вірогідністю будуть відсутні. Також обробка бітового опису трансформанти у напрямку бітових площин доцільна ще й з іншого боку. У цьому випадку може бути забезпечена можливість здійснювати відновлення зображень на прийомному боці за ієрархічним принципом [18-20]. Тоді перший етап, на якому буде здійснюватися декодування зображення (даний етап відповідає обробці елементів бітових старших порядків) дозволить відтворити грубу форма зображення. Відповідно, аналогічним чином на наступних етапах буде виконуватися уточнення зображення аж до одержання відеоданих без похибки. У цьому випадку груба форма зображення буде формуватися на базі бітових площин старших розрядів, які містять у собі інформацію про значення старших розрядів компонент трансформант. У свою чергу, бітовим площинам молодших порядків буде відповідати інформація, що буде уточнювати дані відносно об'єктів зображення.

Далі на базі формули (3) виконаємо запис виразу, який дозволяє обчислити значення коду

$E(q)_m^{(\mu)}$ для m-й послідовності довжин серій двійкових елементів, які було виявлено у межах μ-й бітової площини q-ї трансформанти:

$$E(q)_m^{(\mu)} = \ell_{m,1}^{(\mu)} \prod_{\phi=2}^{\Theta_m}(b_\phi+1)+ ... \\ ...+\ell_{m,\theta}^{(\mu)} \prod_{\phi=\theta+1}^{\Theta_m}(b_\phi+1)+ ... + \ell_{m,\Theta_m}^{(\mu)} = \\ = \sum_{\theta=1}^{\Theta_m} \ell_{m,\theta}^{(\mu)} \prod_{\phi=\theta+1}^{\Theta_m}(b_\phi+1), \quad (5)$$

де $\ell_{m,\theta}^{(\mu)}$ є довжинами θ-ї серії двійкових елементів, що відносяться до m-ї послідовності довжин двійкових елементів, які було виявлено у межах μ-ї бітової площини;

$(b_\theta+1)$ - основа елементу $\ell_{m,\theta}^{(\mu)}$, що розглядається у вигляді елементу НРПЧ;

$\prod_{\phi=\theta+1}^{\Theta_m}(b_\phi+1)$ - ваговий коефіцієнт для довжини θ-ї серії двійкових елементів;

Θ_m - кількість довжин двійкових елементів, що відносяться до m-ї послідовності.

Для зменшення кількості службових даних при цьому доцільним є формування основ НРПЧ для кількох довжин двійкових серій, як це показано наступним виразом:

$$b_\theta = \psi_{bm}(\ell_{m,\theta,1}^{(\mu)},...,\ell_{m,\theta,\varphi}^{(\mu)}), \quad (6)$$

де $\psi_{bm}(\ell_{m,\theta,1}^{(\mu)},...,\ell_{m,\theta,\varphi}^{(\mu)}\}$ - функціональна залежність, що буде визначати величину основи b_θ, яка залежить від довжин двійкових серій;

φ - кількість довжин серій двійкових елементів, для яких виконується побудова спільної основи b_θ.

Щоб мати змогу побудови основи НРПЧ для кількох довжин двійких елементів, тоді, відповідно до виразу (6), буде формуватися двовимірний масив $L_q^{(\mu)}$ довжин двійкових серій, які було виявлено у межах площини БПТ. Отже, тоді знаходження основ позиційних чисел пропонується здійснювати для довжин двійкових серій кожного рядка. Тоді вираз (6) буде переписано.

$$b(q)_\alpha^{(\mu)} = \max\{\ell_{\alpha,1}\ \ell_{\alpha,2}\ ...\ \ell_{\alpha,\beta}\ ...\ \ell_{\alpha,\varepsilon}\}+1, \\ \alpha=\overline{1,\varepsilon}. \quad (7)$$

Тоді опис загального процессу формування кодового опису трансформанти будет таким:

1. Виконання декомпозиції вихідної трансформанти ДКП, у результаті чого буде отримано ν_{pb} бітових площин.

2. Знаходження довжин серій двійкових елементів у межах окремої бітової площини. У цьому випадку можуть розглядатися варіанти обходу бітових площин як у напрямку рядків або стовпців. По мірі виявлення ланцюжків двійкових елементів формується масив $L_q^{(\mu)}$, як показано формулою (7).

3. Визначення основи елемента нерівновагого позиційного числа відповідно до виразу (8).

4. Обчислення вагових коефіцієнтів нерівновагих позиційних чисел як добутків основ, починаючи з $(b_\phi+1)$ -го індексу.

5. Обчислення значення коду нерівновагого позиційного числа відповідно до формули (5).

3. ВИСНОВОК

Запропоновано метод кодування бітового опису трансформанти, заснований на нерівновагових позиційних кодах для усунення структурної надмірності трансформант ДКП. Даний метод орієнтований на застосування у якості базису для технології керування бітовою швидкістю відеопотоку. На відміну від стандартизованих методів кодування, розглянутий метод дозволяє формувати кодовий опис трансформанти у вигляді ряду незалежних кодових конструкцій бітових площин. Це дає можливість у ході керування виключати окремі бітові площини з розгляду, тим самим змінюючи рівень інтенсивності.

4. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] V. V. Barannik, N.A. Kharchenko, V.V. Tverdokhleb, O. Kulitsa, "The issue of timely delivery of video traffic with controlled loss of quality", in *Proceedings of the International Conference on Modern Problems of Radio Engineering. Telecommunications and Computer Science (TCSET),* 2016, pp. 902-904. doi: 10.1109/TCSET.2016.7452220

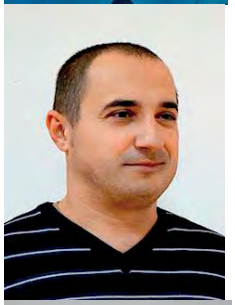
[2] V. Barannik, A. Krasnoruckiy, A. Hahanova, "The positional structural-weight coding of the binary view of transformants", in *Proceedings of the International Conference on East-West Design and Test Symposium (EWDTS),* September 2013, pp. 1-4. doi: 10.1109/EWDTS.2013.6673178

[3] R.C. Gonzales and R.E. Woods. *Digital image processing*, sec. edition. Prentice Hall, New Jersey, 2002, 1072 p.
[4] Ian Richardson, *H.264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia / Ian Richardson*, pp. 368, 2005.
[5] Y. Zhang, S. Negahdaripour and Q. Li, "*Error-resilient coding for underwater video transmission*," OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, 2016, pp. 1-7.
[6] V Barannik, S Podlesny, D Tarasenko, D Barannik, O Kulitsa. "The video stream encoding method in infocommunication systems", in *Proceedings of the International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET),* Lviv, 2018, pp. 538-541, doi: 10.1109/TCSET.2018.8336259
[7] S. Wang, X. Zhang, X. Liu, J. Zhang, S. Ma, W. Gao, "Utility-Driven Adaptive Preprocessing for Screen Content Video Compression", *IEEE Transactions on Multimedia*, vol. 19, no. 3, pp. 660-667, 2017.
[8] H. Baccouch, P. L. Ageneau, N. Tizon, N. Boukhatem, "Prioritized network coding scheme for multilayer video streaming", in *Proceedings of the International Conference on 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2017, pp. 802-809,
[9] W. J. Tsai, Y. C. Sun, "Error-resilient video coding using multiple reference frames", in *Proceedings of the International Conference on IEEE International Conference on Image Processing*, 2013, pp. 1875-1879.
[10] Shi, Yun Q. *Image and video compression for multimedia engineering: fundamentals, algorithms, and standards*. CRC Press, NY, 2008, 576 p.
[11] K. R. Rao and J. J. Hwang. *Techniques and Standards for Image, Video and Audio Coding*. EnglewoodCliffs, NJ: Prentice-Hall, 1996.
[12] Ablamejko S.V., Lagunovskij D.M. *Obrabotka izobrazhenij: tehnologija, metody, primenenie*. Amalfeja, Minsk, 2000, 303 p.
[13] Ding Z., Chen H., Gua Y., Peng Q. *GPU accelerated interactive space-time video matting*. In Computer Graphics International P 163-168. 2010.
[14] Christophe E., Lager D., Mailhes C. "Quality criteria benchmark for hiperspectral imagery", *IEEE Transactions on Geoscience and Remote Sensing*. Vol. 43. No 9. pp. 2103–2114, 2005.
[15] Lee S. Y. Yoon J. *C. Temporally coherent video matting. Graphical Models 72*. 2010. P. 25-33.
[16] Vatolin D., Ratushnyak A., Smirnov M. and Yukin V. *Methods of data compression. The device archiver, compression of images and videos.* M. Dialog Mifi, 2013, 384 p.
[17] D. Salomon. *Data Compression: The Complete Reference.* Fourth Edition. Springer-Verlag London Limited, 2007, 899 p.
[18] V.V Barannik., Yu.N. Ryabukha, S.A Podlesnyi. "Structural slotting with uniform redistribution for enhancing trustworthiness of information streams", *Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika)*, №76 (7), pp.607, 2017. doi: 10.1615 / TelecomRadEng.v76.i7.40.
[19] A.N. Alimpiev, V.V. Barannik, S.A. Sidchenko "The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space", *Telecommunications and Radio Engineering, English translation of Elektrosvyaz and Radiotekhnika*, №76 (6), pp. 521-534, 2017, doi: 10.1615/TelecomRadEng.v76.i6.60.
[20] A. Chigorin, G. Krivovyaz, A. Velizhev, A. Konushin. "A method for traffic sign detection in an image with learning from synthetic data", in *Proceedings of the International Conference on Digital Signal Processing and its Applications*, 2012, pp. 316-335.

***Бараннік Володимир Вікторович**, начальник кафедри бойового застосування та експлуатації АСУ ХНУПС. Область наукових інтересів – кодування та обробка даних*

***Рябуха Юрій Миколайович**, професор ХНУПС. Область наукових інтересів – кодування та обробка даних*

***Гуржій Павло Миколайович,** начальник науково-дослідного відділу наукового центру ВІТІ*



***Твердохліб Віталій Вікторович,** асистент кафедри інформаційно-мережної інженерії ХНУРЕ. Область наукових інтересів – обробка мультимедійних даних*

***Шевченко Ігор Олександрович,** здобувач кафедри інформаційно-мережної інженерії ХНУРЕ. Область наукових інтересів – обробка мультимедійних даних*

DOI: https://doi.org/10.17721/ISTS.2019.1.57-65
УДК 004.9: 621.391.7

СИНТЕЗ МЕТОДІВ ОЦІНЮВАННЯ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ РАДІОТЕХНІЧНИХ СИСТЕМ

Лукова-Чуйко Наталія [1]
orcid.org/0000-0003-3224-4061

Наконечний Володимир [2]
orcid.org/0000-0002-0247-5400

Сайко Володимир [3]
orcid.org/0000-0002-3059-6787

Толюпа Сергій [4]
orcid.org/0000-0002-1919-9174

[1] м. Київ, Київський національний університет імені Тараса Шевченко, lukova@ukr.net
[2] м. Київ, Київський національний університет імені Тараса Шевченко, nvc2006@i.ua
[3] м. Київ, Київський національний університет імені Тараса Шевченко, tolupa@i.ua
[4] м. Київ, Київський національний університет імені Тараса Шевченко, vgsaiko@gmail.com

Історія статті:

Надійшла до редакції 17.06.2019
Прийнято 11.08.2019

Ключові слова:
електромагнітне поле, електромагнітна сумісність; навмисні перешкоди; радіотехнічна система; радіоелектронні засоби; умови електромагнітної сумісності.

Анотація: Сучасний розвиток радіотехнічних засобів характеризується зростанням швидкодії процесів передачі й обробки інформації, мініатюризацією та інтеграцією в єдині комплекси, що фізично зближує джерела і рецептори перешкод. Все це призводить до посилення вимог щодо забезпечення виконання умов електромагнітної сумісності і до необхідності її оцінювання на стадії проектування радіотехнічних пристроїв і систем. Неповна або невірна оцінка цих вимоги приводить до значного зростання часових і матеріальних витрат виробника, на подальше доопрацювання розроблювальної електронної апаратури і зниження її конкурентоспроможності. Широке використання різних за призначенням радіоелектронних засобів призводять до зростання рівнів електромагнітних полів, що створюються ними в навколишньому просторі. Ці поля є перешкодами для інших подібних пристроїв, можуть погіршувати умови функціонування і знижувати ефективність їх застосування. Цей процес має характерні риси діалектичного розвитку - прогрес в цій області стримується негативними явищами, породженими її розвитком. Подальший прогрес вимагає подолання цієї тенденції, тобто розвитку на новому якісному рівні, що полягає в забезпеченні спільного функціонування різних електронних засобів. Принциповим є те, що дії електромагнітних полів, які створюються одними технічними засобами на інші, здійснюються для передачі інформації, її обробки, або навпаки, порушення процесу передачі і обробки даних. Тому в роботі запропонований відповідний аналіз, що дозволяє проводити попереднє прогнозування виконання умов електромагнітної сумісності в групі радіоелектронних засобів, які мають деяке число джерел перешкод і радіотехнічних пристроїв на які вони впливають. При цьому, важливим питанням перевірки забезпечення електромагнітної сумісності радіоелектронних засобів є визначення величини припустимої потужності при якій забезпечується умова електромагнітної сумісності. Метою даної статті є розгляд, із загальних позицій, основних завдань аналізу та оцінювання електромагнітної сумісності радіоелектронних засобів.

Abstract: Modern development of radio equipment is characterized by an increase in the speed of processes of transmission and processing of information, miniaturization and integration into unified complexes that physically bridles the sources and receptors of interference. All this leads to the strengthening of the requirements to ensure compliance with the conditions of electromagnetic compatibility and the need for its evaluation at the design stage of radio engineering devices and systems, because the incomplete or incorrect assessment of these requirements leads to a significant increase in time and material costs of the manufacturer, for further development of the development of electronic equipment and reduction its competitiveness. Widespread use of different purposeful electronic means leads to an increase in the levels of electromagnetic fields created by them in the surrounding space. These fields are obstacles for

other similar devices, may degrade the operating conditions and reduce the effectiveness of their use. In this process, it is easy to see the characteristic features of dialectical development - progress in this area is restrained by the negative phenomena generated by its development. Further progress requires the overcoming of this trend, that is, development on a new quality level, which is to ensure the joint operation of various means. The key is that the actions of the electromagnetic fields, which are created by some technical means to the other, are carried out for the transmission of information, its processing, or vice versa, violation of the process of transmission and processing of data. Therefore, an analysis is proposed that allows preliminary prediction of the fulfillment of the conditions of electromagnetic compatibility in a group of radio-electronic means that have a number of sources of interference and radio engineering devices on which they affect. In this case, the important issue of checking the provision of electromagnetic compatibility of radio-electronic means is to determine the magnitude of the permissible power at which provides electromagnetic compatibility. The purpose of this article is to consider, from the general positions, the main tasks of the analysis and evaluation of the electromagnetic compatibility of radio-electronic means

.

1. ВСТУП

Широке використання різних за призначенням радіоелектронних засобів (РЕЗ) призводять до зростання рівнів електромагнітних полів, що створюються ними в навколишньому просторі. Такі поля є перешкодами для інших подібних пристроїв, вони можуть погіршувати умови їх функціонування і знижувати ефективність застосування.

Сучасний розвиток радіотехнічних засобів (РТЗ) характеризується зростанням швидкодії процесів передачі й обробки інформації, мініатюризацією та інтеграцією в єдині комплекси, що фізично зближує джерела і рецептори перешкод. Все це призводить до посилення вимог щодо забезпечення виконання умов електромагнітної сумісності (ЕМС) і до необхідності її оцінювання на стадії проектування радіотехнічних пристроїв і систем. Неповна або невірна оцінка цих вимоги приводить до значного зростання часових і матеріальних витрат виробника, на подальше доопрацювання розроблювальної електронної апаратури і до зниження її конкурентоспроможності.

Усе це загострює проблему забезпечення виконання умов ЕМС, яка має виражений системний характер. При оцінюванні ЕМС радіоелектронних систем (РЕС) мають розглядатися завдання внутрішньо-системної оцінки ЕМС, коли враховуються ненавмисні перешкоди (НеП), що створюються засобами конкретного об'єкту, а також завдання міжсистемного оцінювання ЕМС, коли в якості джерел перешкод розглядаються різні типи існуючих РЕС.

– я ЕМС при переміщенні РЕС і зміні умов їхньої експлуатації;

– відпрацювання варіантів заходів щодо

Оцінювання ЕМС радіотехнічних засобів є загальним завданням, з яким доводиться контактувати на різних етапах життєвого циклу РТЗ різного призначення і типу. Тому на стадії планування і проектування РТЗ актуальність проблеми ЕМС не зменшується. Це обумовлено збільшенням концентрації РЕЗ в обмеженому просторі, розширенням їх типажу і підвищенням ролі радіоелектронних засобів, при розв’язанні найрізноманітніших завдань. При цьому відсутність оцінювання вимог ЕМС на стадії планування і проектування виробу приводить до серйозних труднощів щодо забезпечення безперешкодної роботи РЕС на подальших стадіях їх життєвого циклу.

На стадії проектування виробу має проводитися всебічне оцінювання ЕМС засобів, що розробляються з усіма існуючими, які можуть використовуватися спільно на одній території. При цьому, оцінювання ЕМС має проводитися з урахуванням усього комплексу РЕЗ об'єкту і з урахуванням умов їхнього застосування за призначенням.

При випробуваннях зразків РЕС, в основному, застосовується експериментальний метод оцінювання ЕМС, проте, використовуються також і теоретичні методи. Найгостріше проблема ЕМС відчувається на етапі експлуатації радіоелектронних систем. На цьому етапі виникають численні завдання щодо забезпечення безперешкодної роботи РЕС. До таких завдань можна віднести:

– оцінювання ступеня забезпечення ЕМС при розміщенні РЕЗ на об'єктах (БПЛА, автомобілях, кораблях і т. п.) і місцевості;

– прогнозуванн

забезпечення умов виконання ЕМС РЕС і т. і.

Проблема ЕМС особливо актуальна для мобільних РТС, на повітряних, наземних, або

водних носіях, у складі яких передбачається одночасне застосування різних засобів радіолокації та телекомунікації. Виходячи з того, що РТС є складними і багатовимірними системами слідує необхідність системного розгляду питання ЕМС і її компонентів. Такий системний аналіз забезпечення ЕМС має базуватися на єдиному підході до усіх її складових частин з урахуванням взаємного впливу їх один на одного і на систему в цілому.

На практиці це припускає використання системного підходу до забезпечення ЕМС РЕС, починаючи з ранніх етапів життєвого циклу, а саме, при виборі концепції їх побудови, у ході схемотехнічного, конструкторського і технологічного проектування, а також у ході процесу виробництва з урахуванням використання засобів активного контролю.

Усе це визначило актуальність, важливість і практичну значущість вирішуваної в цій статті науково-технічної задачі - оцінювання виконання умов ЕМС РТС, у тому числі її підсистем, локалізованих в обмеженому просторі.

2. Постановка проблеми

Проблема електромагнітної сумісності має два аспекти, що доповнюють один одного. Будь-яка ситуація електромагнітної несумісності повинна мати джерело перешкод і рецептор, який чутливий до цих перешкод. Якщо одна з цих складових відсутня, то відсутня і проблема ЕМС. Є також і третій чинник - зв'язок між джерелом і рецептором, який може бути безпосереднім, при їх близькості, або за допомогою енергії випромінювання. Деякі пристрої в одній ситуації можуть бути джерелами перешкод, і рецепторами в іншому випадку.

Проблема ЕМС РТС є певною конкретизацією відомої проблеми завадозахищеності РЕЗ. Фундаментальні роботи Котельникова В.А., Гуткіна Л.С., Тихонова В.І., Трифонова А.П. і багатьох інших учених, які працюючи над загальними завданнями завадостійкості радіоприймальних пристроїв, підготували велику теоретичну базу для розв’язання багатьох конкретних завдань ЕМС РТС [1-5].

Проте, проблема забезпечення ЕМС радіоелектронних засобів ставить нові задачі, що визначаються специфікою їх спільної роботи. В загальному випадку розв’язання проблеми ЕМС нині проводиться за двома напрямками: організаційними і технічними заходами.

Організаційні заходи застосовуються, в основному, для захисту від НеП, що створюються "своїми" джерелами. Завдання забезпечення ЕМС радіотехнічних засобів має розглядатися, як завдання оптимізації спільної роботи структури і властивостей усього комплексу РТЗ. Зокрема, розв’язання проблеми може зводитися до завдання оптимізації просторового розташування РТЗ, регламентації використання частотного діапазону, а також задачі оптимального управління параметрами сигналів і характеристик РЕЗ [5-6].

Технічні заходи захисту від неумисних і організованих перешкод передбачають впровадження дієвих заходів індивідуального захисту радіоприймальних пристроїв (РПрП). Проведення відповідних організаційних і технічних заходів, створюють умови для недопущення перешкод від передавальних засобів на вхід приймальних пристроїв за рахунок їх синхронізації, або проведення жорсткої регламентації використання часового і частотного ресурсу. Проте, при цьому не вирішується проблема захисту від перевіддзеркалення власного випромінювального сигналу і прийому імпульсів "своїх" РЕЗ, не охоплених організаційними заходами, а також від організованих перешкод різної структури і інтенсивності.

3. Виклад основного матеріалу

Сучасні РЕЗ до певної міри захищені від стандартного набору небезпечних перешкод, розроблених ще у 60-70 роках минулого століття. Проте, в останні роки можливості систем радіоелектронної боротьби (РЕБ) істотно зросли. Насамперед, за рахунок впровадження елементів цифрової техніки з'явилася можливість формувати ефективні сигналоподібні перешкоди, що ускладнюють або блокують процес спостереження РЛС в режимі огляду і призводять до зриву режимів автоматичного супроводження об’єктів. Крім того використання цифрових каналів зв'язку відкрило новий напрям радіоелектронного пригнічення, як в спеціальних сферах їх застосування, так і для каналів загального користування. Це так звані імітаційні перешкоди, які дозволяють несанкціоновано впливати, як на засоби обробки сигналів у приймальному тракті каналу зв'язку, так і на системи тактової і циклової синхронізації [7].

Захист від радіоперешкод різної природи і інтенсивності базується на відмінності структури і закономірностей зміни параметрів, властивих корисним сигналам і діям, що заважають. Це забезпечується захистом від перевантажень приймачів, селекцією сигналу від перешкод, компенсацією перешкод, використанням адаптивних методів захисту. На теперішній час у сучасних бортових РЛС для боротьби з локальними перешкодами застосовують

некогерентні компенсатори, що забороняють проходження сигналів перешкод, якщо їх значення в основному каналі прийому менше значення в компенсаційному каналі з не напрямленою антеною [8]. Проте, використання принципу заборони призводить до того, що разом із сигналами перешкод пригнічуються і корисні сигнали, відбиті від реальних об'єктів. Пригнічення перешкод можливе лише при значному кутовому рознесенні об'єктів і постановника перешкод.

Одним з ефективних способів боротьби з розподіленими в просторі перешкодами в однопозиційних РЛС є формування провалів (нулів) діаграми спрямованості антени в напрямі на постановників перешкод, що реалізовується за допомогою адаптивних фазованих антенних решіток, або широко вживаних в наземних і корабельних РЛС автокомпенсаторів бічних пелюсток антени [7-9].

В реальних умовах "нулі" діаграми спрямованості антени бортової РЛС мають кінцеве значення. Як наслідок, при високому потенціалі станцій активних перешкод, що забезпечується потужним передавачем і фазованими антенними решітками із спрямованим випромінюванням, можливі ситуації, коли залишки перешкод, що не компенсуються, перевищуватимуть за потужністю сигнал відбитий від об'єкта спостереження. Це може привести до пригнічення сигналу від об'єкту, або появи неправдивих відміток на індикаторі в тих напрямах, де об'єкт відсутній. Деякі, існуючі нині, способи захисту бортових РЛС від організованих перешкод описані в [7-9]. Додаткові можливості у боротьбі з

чи виграш при обробці за рахунок кореляційного стискання спектру прийнятого корисного сигналу в смузі модулюючих частот при одночасному розширенні спектру перешкоди.

До сучасних методів захисту цифрових РЕЗ від адитивних перешкод, а також від мультиплікативних перешкод можна віднести використання оптимальних (квазіоптимальних) алгоритмів демодуляції цифрового сигналу, вибір оптимальної структури сигналу, а також використання адаптивних завадостійких кодів, узгоджених з каналом зв'язку [8, 10, 11].

Для захисту ШССЗ від коливань, що заважають, рівень яких перевищує забезпечуваний базою припустимий запас завадостійкості (рівень імовірності помилки на біт), застосовують різні методи пригнічення перешкод, які можна розділити на дві групи [8-10]:

сигналоподібними і багатоточковими перешкодами з'являються при організації колективного захисту від завад у рамках багатопозиційних радіолокаційних систем.

Останніми роками значний прогрес в РТС та телекомунікаційних технологіях досягнутий завдяки переходу на цифрові види зв'язку і обробки інформації з використанням сучасних видів модуляції. Проте, проблеми захищеності від завад і ЕМС існують і в сучасних системах зв'язку. Істотні радіочастотні перешкоди, властиві усім бездротовим системам і є одним з найбільш важливих параметрів в системах мобільного зв'язку. Неумисні і організовані перешкоди різної інтенсивності можуть проникати в системи радіозв'язку, як по основному, так і по побічних каналах прийому [9-11]. Одним із шляхів підвищення завадостійкості РТС зв'язку, радіолокації і радіонавігації є застосування широкосмугових шумоподібних сигналів, що формуються на основі технології розширення спектру (Spread Spectrum, SS) [10, 11]. Розширення спектру є метод формування сигналу за допомогою додаткового ступеня модуляції, що забезпечує не лише розширення спектру сигналу, але і послаблення його впливу на інші сигнали [12, 13].

Широкосмугові системи зв'язку (ШССЗ) знаходять застосування завдяки своїм потенційним перевагам [9, 10]. При роботі в лінійному режимі, системи з розширенням спектру забезпечують істотне пригнічення, як перешкод з вузькою смугою частот (зокрема, гармонійних), так і широкосмугових перешкод забезпечую

- режекція ураженої частини спектру шумоподібного сигналу (ШПС);
- компенсація перешкоди в РПрП шляхом створення її копії з подальшим відніманням створеної копії перешкоди з вхідного сигналу.

Реалізація цих методів захисту здійснюється, в основному, цифровим способом на проміжній або відео частоті РПрП. При цьому вважають, що вхідні НВЧ каскади РПрП перетворять вхідну суміш корисного сигналу, шуму і перешкод лінійно, не вносячи значних спотворень в сигнал, що підлягає обробці.

В умовах зростаючої кількості працюючих РТС бездротового зв'язку, виникають ситуації, коли рівень перешкод, що надходить на вхід ШССЗ, перевищує можливості динамічного діапазону (ДД) вхідних каскадів РПрП. Аналогічна ситуація можлива у разі цілеспрямованого пригнічення діючої ШССЗ потужною вузькосмуговою перешкодою (ВП).

У цьому випадку вхідні НВЧ каскади ПрП, а саме малошумливий підсилювач (МШП) і змішувач переходять в нелінійний режим роботи. Спотворення корисного ШПС, що виникають внаслідок нелінійних перетворень у вхідних каскадах ПрП, неможливо компенсувати подальшою цифровою обробкою, оскільки характер таких спотворень важко передбачуваний. Отже, виникає необхідність додаткового захисту вхідних каскадів ШССЗ від дії потужних перешкод.

Виходячи з того, що до основних критеріїв ефективності сучасних РТС належать мобільність і здатність функціонувати з високими якісними показниками в умовах невизначеної складної завадової обстановки і часу, наближеного до реального необхідно, щоб така РТС була розміщена на швидкісних повітряних носіях в якості яких можна застосовувати, наприклад, БПЛА. За допомогою таких комплексів набагато ефективніше і дешевше розв’язуються завдання, як дистанційного моніторингу важкодоступних районів, в яких отримання інформації звичайними засобами, включаючи авіарозвідку, ускладнене або ж наражає на небезпеку життя людей. Виміряна інформація в режимі реального часу з БПЛА має передаватися на пункт управління для обробки та ухвалення відповідних рішень [14, 15].

Перераховані вимоги, що покладаються на БПЛА, неможливі без розв’язання ряду науково-технічних завдань спрямованих на [16]:

- підвищення корисного навантаження БПЛА;
- розробку сучасної, легкої і надійної апаратури на базі мікро, нано та піко технологій сприяючи підвищенню ефективності управління БПЛА, збору і передачі інформації на пункти її обробки;
- покращення функціонування БПЛА в умовах невизначеності пов'язаної з ЕМС різних радіоелектронних засобів, як зовнішніх, так і таких, що знаходяться на їхньому борту.

Як правило, перші два класи завдань вирішуються комплексно. Підвищення навантажувальної здатності БПЛА дозволяє встановлювати на його борту додаткову сучасну апаратуру на основі використання метаматеріалів та нанотехнологій, що у свою чергу, підвищує ефективність і розширює коло вирішуваних БПЛА завдань [17].

Розв’язання третього завдання пов'язане з труднощами аналізу ЕМС різних за призначенням РЕЗ, причинами виникнення ненавмисних перешкод, чинниками, що визначають їх поширення і схильність РЕЗ до їхнього впливу. Дія навмисних перешкод (НаП) може суттєво погіршити якість і ефективність функціонування РЕЗ. Тому метою даної статті є розгляд, із загальних позицій, основних завдань аналізу та оцінювання ЕМС до числа яких відносять [16, 18, 19]:

- аналіз електромагнітної обстановки (ЕМО), під якою розуміється сукупність електромагнітних полів, що існують у визначеній області простору і які характеризуються розподілом їх інтенсивності за частотою і часом. Залежно від конкретного випадку може йтися про ЕМО на об'єкті (приміщення, корабель, літак і т. ін.), в конкретному місці, районі, області і т. п.;
- аналіз виконання умов ЕМС у групі засобів на різних етапах життєвого циклу РЕЗ;
- аналіз параметрів ЕМС технічних засобів.

Основним змістом завдань цієї групи є методи і засоби отримання кількісної інформації про відповідність параметрів різних РЕЗ нормативно-технічної документації в області ЕМС.

Для розв’язання другої та третьої груп завдань використовуються:

- аналітичні методи аналізу, реалізовані у вигляді пакетів програм, для завдань прогнозування ЕМС;
- методи фізичного і математичного (імітаційного) моделювання, для оцінювання параметрів ЕМС (рівнів допустимих перешкод);
- експериментальні методи, для визначення параметрів ЕМС, а також на завершальній стадії створення різних радіоелектронних комплексів, завершальних випробуваннях у ході яких в числі інших показників здійснюється і контроль виконання умов ЕМС.

4. РЕЗУЛЬТАТИ

Метою аналізу ЕМС в групі радіоелектронних засобів є прогноз виконання умов, при яких забезпечується електромагнітна сумісність в деякій сукупності РЕЗ, що містить джерела перешкод $N_{\text{ДП}}$ і рецепторів $N_{\text{РП}}$.

В основу здійснення аналізу покладене наступне. Кожний технічний засіб, що є рецептором перешкод, призначений для певних функцій і характеризується показником якості $Q_{\text{РП}}$, що відображає їх виконання. Під дією перешкоди *i*-го типу якість виконання цих функцій знижується, що можна представити як зменшення значення $Q_{\text{РП}}(P_{\text{РП}})$ (рис. 1).

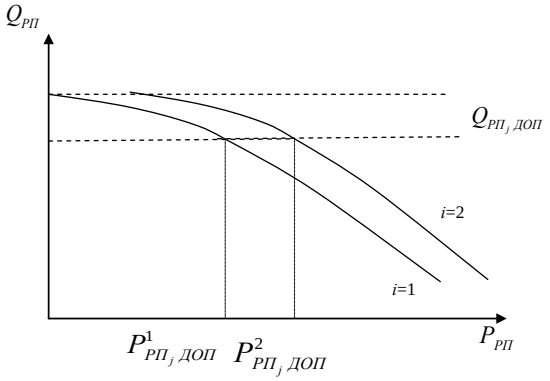


Рис. 1 - Графіки залежностей показників якості виконання функцій від дії *i*-го джерела перешкоди

Допустимому зниженню якості $Q_{\text{РП}}$ відповідає перешкода *i*-го виду з рівнем не більше $P^1_{\text{РП}_j\ \text{ДОП}}$. Перешкоди, при яких не відбувається неприпустимого зниження якості функціонування *i*-го рецептора, називають допустимими. При цьому, рівні допустимих перешкод *j*-му рецептору розрізняються залежно від спектрального складу і часових характеристик перешкоди *i*-го виду. Тому для різних видів перешкод значення $P^i_{\text{РП}_j\ \text{ДОП}}$ також різні.

Припустимо, що вказані величини для *j*-го рецептора відомі. У цьому випадку принцип аналізу виконання умови ЕМС у групі засобів полягає в знаходженні величин $P^1_{РП_j}$ і порівнянні їх з допустимими значеннями. Це може бути виконано на різній основі. Розрізняють наступні способи здійснення такого аналізу: парну, групову [20] й запропановану комплексно-групову оцінки [17].

При методі парного оцінювання по черзі розглядається дія кожного з $N_{ДП}$ джерел на перший рецептор, потім на другій і так далі (рис. 2).

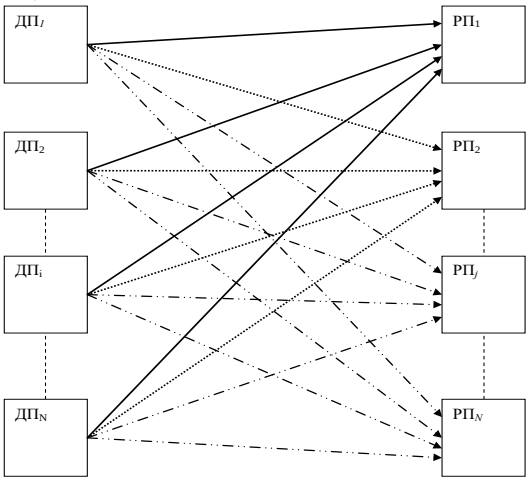


Рис. 2 - Метод парного оцінювання ЕМС РЕЗ

Таким чином, здійснюється почергова перевірка ЕМС кожного з джерел з кожним з рецепторів за критерієм допустимого зниження якості функціонування:

$$Q_{\text{РП}_j}(P_{\text{РП}_j}) \geq Q^i_{\text{РП}_j\text{ДОП}} \rightarrow \text{ЕМС}.$$

$$Q_{\text{РП}_j}(P_{\text{РП}_j}) < Q^i_{\text{РП}_j\text{ДОП}} \rightarrow \text{порушення ЕМС},$$

або по рівню завад від *i*-го джерела, що діє на *j*-й рецептор:

$$P_{\text{РП}_j}(P_{\text{ДП}_i}) \leq P^i_{\text{РП}_j\text{ДОП}} \rightarrow \text{ЕМС}\ \ (j \leftarrow i), \quad (1)$$

$$P_{\text{РП}_j}(P_{\text{ДП}_i}) > P^i_{\text{РП}_j\text{ДОП}} \rightarrow \text{порушення ЕМС}.$$

Метод парного оцінювання є найбільш простим у здійсненні, але в той же час не завжди вірогідним, оскільки не дозволяє враховувати повною мірою такі явища, як інтермодуляція тобто взаємодію між двома або більше частотами, що проходять через активний або пасивний нелінійний електричний ланцюг, або через будь-який компонент, який генерує небажані частоти, як у приймачі, так і інтермодуляційне випромінювання передавачів.

Більш вірогідним є метод групового оцінювання, при якому розглядаються по черзі дія кількох джерел $N_{\text{ДП}}$ на кожний з рецепторів у групі (рис. 3).

При методі групового оцінювання виходять з того, що якість функціонування *j* - го рецептора $Q_{РП_j}$ залежить від рівнів перешкод, які створюються рядом джерел:

$$Q^K_{\text{РП}_j} = Q_{\text{РП}}(P_{\text{РП}_K} \ldots P_{\text{РП}_{K+N_{\text{ДП}}}}).$$

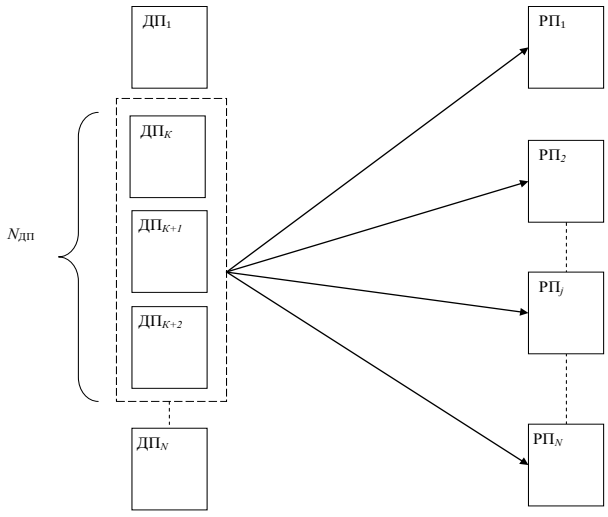


Рис. 3 - Метод групового оцінювання ЕМС РЕЗ

Відповідно факт виконання або невиконання умов ЕМС перевіряється по зниженню якості кожного з $РП_N$ рецепторів з кожною з груп джерел:

$$Q^{K}_{\text{РП}_j} \geq Q_{\text{РП}_j\text{ДОП}} \rightarrow \text{ЕМС}\ (j \leftarrow N_{\text{ДП}});$$

$$Q^{K}_{\text{РП}_j} < Q_{\text{РП}_j\text{ ДОП}} \rightarrow \text{порушення ЕМС}.$$

Метод групового оцінювання дозволяє враховувати вплив всіляких ефектів, пов'язаних з позасмуговими ефектами в рецепторах і інтермодуляцію в джерелах перешкод. Платою за це є підвищення трудомісткості розрахункових процедур.

Незважаючи на велику міру адекватності і реальності, деякі аспекти забезпечення ЕМС у групі засобів і при груповому оцінюванні залишаються поза увагою. В основному це стосується комплексів технічних засобів, що складаються із різних джерел і рецепторів перешкод і при цьому розв’язують деяку загальну для усієї групи задачу.

Для якомога повнішої оцінки впливу різних ефектів, що з'являються в приймально-передавальних і сигнальних трактах РЕЗ запропоновано метод комплексно-групового оцінювання ЕМС радіоелектронних засобів.

При методі комплексно групового оцінювання ЕМС РЕЗ розглядається група радіотехнічних засобів, що виконують різні функції, спрямовані на досягнення деякої загальної для усієї групи мети (рис. 4).

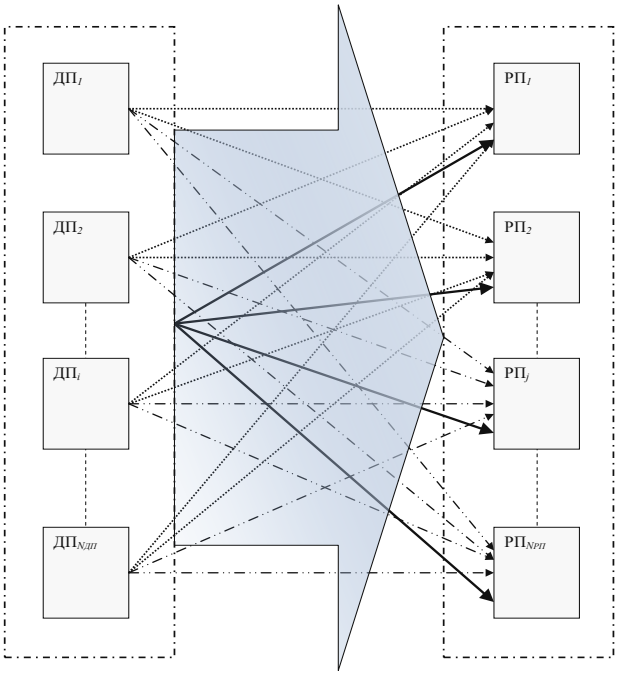


Рис. 4 - Метод комплексно групового оцінювання ЕМС РЕЗ

Розглянемо метод комплексно групового оцінювання детальніше. Нехай величина Q_{Σ} характеризує якість функціонування групи рецепторів, що вирішує загальну задачу:

$$Q_{\Sigma} = Q_{\Sigma}\left(Q_{\text{РП}_1} \ldots Q_{\text{РП}_j} \ldots Q_{\text{РП}_N}\right),$$

причому кожен з частинних показників якості окремих рецепторів залежить від рівнів перешкод, що діють з боку усієї групи джерел (аналогічно груповому оцінюванні).

Виконання або порушення умов ЕМС визначається за критерієм допустимого зниження якості функціонування для групи рецепторів у цілому:

$$Q^{K}_{\Sigma} \geq Q^{K}_{\Sigma\text{ДОП}} \rightarrow \text{ЕМС}\ (N_{\text{РП}} \leftarrow N_{\text{ДП}});$$

$$Q^{K}_{\Sigma} < Q^{K}_{\Sigma\text{ДОП}} \rightarrow \text{порушення ЕМС}.$$

Метод комплексно групового оцінювання дозволяє судити про виконання або порушення ЕМС у групі засобів, що виконують загальне завдання, коли зниження якості функціонування окремих складових не дає повної картини впливу ненавмисної електромагнітної перешкоди на результат спільної роботи цих складових.

Прикладом аналізу методом комплексно групового оцінювання ЕМС РЕЗ може служити сукупність підсистем на борту сучасного БПЛА, що включає засоби, навігації, радіолокації, зв'язку, канал розпізнавання і т. ін.

Інформація про погіршення показників цих підсистем під дією НеП не дає сама по собі повної картини впливу перешкод на результат виконання поставленого загального завдання, наприклад моніторингу повітряної або наземної обстановки та розпізнавання виявлених об'єктів.

Проведемо розгляд процедури отримання парного оцінювання ЕМС в групі засобів.

Здійснення метода парного оцінювання може проводитися, як на основі детермінованого підходу, так і ймовірнісного. При детермінованому підході усі величини, що визначають значення $P^{i}_{\text{РП}_j}$, вважаються детермінованими і перевірка виконання умови ЕМС полягає в порівнянні величини $P^{i}_{\text{РП}_j}$ з допустимим значенням.

Рішення щодо електромагнітної сумісності приймається при перевірці виконання умови:

$$P^{i}_{\text{РП}_j} > P^{i}_{\text{РП}_j\text{ДОП}} \rightarrow \text{порушення ЕМС}.$$

Існує ряд вагомих причин щодо яких реальне використання детермінованого підходу може привести до незадовільних (часто надмірно завищених) результатів:

- апріорна недостатність інформації про значення параметрів, що визначають значення $P^{i}_{\text{РП}_j}$;

- зміна параметрів ЕМС внаслідок впливу температурних, кліматичних чинників, старіння

елементів і т. ін.;

- робота технічних засобів, в різних динамічних ситуаціях, коли змінюються відстані між засобами, їх взаємна орієнтація, зміна частотних каналів і так далі.

В усіх перерахованих випадках результатом є те, що при детермінованому підході або розглядається найгірший випадок, що призводить до надмірно жорстких оцінок, або використовуються деякі усереднені показники, які не дозволяють контролювати міру вірогідності оцінок.

Імовірнісний підхід дозволяє в подібних випадках істотно підвищити вірогідність оцінки виконання умов ЕМС. Згідно з імовірнісним підходом чинники, що визначають потужність перешкоди $P^i_{\text{РП}_j}$ і відповідно її значення, вважаються випадковими величинами. Факт виконання умови ЕМС $P^i_{\text{РП}_j} \le P^i_{\text{РП}_j\text{ДОП}}$ також розглядається як випадкова подія, ймовірність якої дорівнює:

$$P^{i,j}_{\text{СУМ}} = \int_{o}^{P^i_{\text{РП}_j\text{ДОП}}} W(P^i_{\text{РП}_j})dP^i_{\text{РП}_j}, \qquad (2)$$

де $W(P^i_{\text{РП}_j})$ - щільність розподілу величини $P^i_{\text{РП}_j}$.

Згідно з імовірнісним підходом умова ЕМС *j*-го рецептора з *i*-м джерелом перешкод вважається виконаю, якщо ймовірність порушення ЕМС $P^{i,j}_{\text{ПОР}} = 1 - P^{i,j}_{\text{СУМ}}$ мала, тобто не перевищує деякого припустимого значення $P^{i,j}_{\text{ПОР}\,ПРИП}$.

З іншого боку величина $P^i_{\text{РП}_j}$ розглядається як випадкова та характеризується середнім значенням $m(P^i_{\text{РП}_j})$ і середньоквадратичним відхиленням (СКВ) - $\sigma(P_{\text{РП}_{ij}})$.

Як відомо з теорії ймовірності, відхилення випадкової величини від її середнього значення на величину, що перевищує декілька значень СКВ, малоймовірні. Отже, відповідно до ймовірнісного підходу умова ЕМС вважається виконаною, якщо:

$$m(P^i_{\text{РП}_j}) + \xi\sigma(P_{\text{РП}_{ij}}) \le P^i_{\text{РП}_j\,\text{ПРИП}}, \qquad (3)$$

де величина ξ визначається припустимою ймовірністю порушення ЕМС $\xi = \xi(p^{i,j}_{\text{ПОР ПРИП}})$.

Згідно до ймовірнісного підходу для кожної *i, j*-ої пари засобів оцінюють середні значення $m(P^i_{\text{РП}_j})$ і середньоквадратичні відхилення $\xi\sigma(P_{\text{РП}_{ij}})$ величини потужності перешкоди, що діє на *j*-й рецептор від *i*-го джерела, і порівнюють їх зважену суму (3) з рівнем допустимої перешкоди.

5. ВИСНОВКИ

Таким чином, запропонований аналіз дозволяє проводити попереднє прогнозування виконання умов ЕМС в групі радіоелектронних засобів, які мають деяке число джерел перешкод і радіотехнічних пристроїв на які вони впливають. При цьому, важливим питанням перевірки забезпечення ЕМС РЕЗ є визначення величини припустимої потужності $P^i_{\text{РП}_j\,\text{ПРИП}}$ при якій забезпечується ЕМС.

6. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Котельников В.А. Теория потенциальной помехоустойчивости / В.А. Котельников. - М: Радио и связь, 1998. - 400 с.

[2] Гуткин Л.С. Теория оптимальных методов радиоприёма при флуктуационных помехах / Л.С. Гуткин. - М.: Сов. радио, 1972. - 487 с.

[3] Тихонов В.И. Помехоустойчивость оптимальных методов приёма фазомодулированных и частотно-модулированных радиосигналов / В.И. Тихонов // Электросвязь. - 1969. - № 3. - С. 25-32.

[4] Трифонов А.П. Совместное различение сигналов и оценка их параметров на фоне помех / А.П. Трифонов, Ю.С. Шинаков. - М.: Радио и связь, 1986. - 286 с.

[5] Вазин В.А. Оптимизация характеристик ЭМС РТС путем автоматического управления ее параметрами / В.А. Вазин, В.Р. Железцов, В.М. Соловьев // Радиоизмерительная аппаратура для решения задач ЭМС РЭС: Межвузовский сб., Горький, Горьк. гос. ун-т. - 1989. - С. 30-34.

[6] Силин А.В. Оценка ЭМС в комплексе РЭС святи / А.В. Силин // Радиоизмерительная аппаратура для решения задач ЭМС РЭС: Межвузовский сб., Горький, Горьк. гос. ун-т. - 1989. - С. 98-109.

[7] Орощук И.М. Новые технологии радиоэлектронного подавления каналов автоматизированных систем радиосвязи / И.М. Орощук. - Владивосток, ТОВМИ им С.О.Макарова, 2000. - 368 с.

[8] Резонансні методи отримання і використання інформації в радіотехнології: Монографія / В.А. Дружинін, І.Р. Пархомей, С.В. Толюпа, В.С. Наконечний. - К.: Логос, 2013. - 146 с.

[9] Методи та алгоритми обробки радіолокаційної інформації в багатопозиційних системах зі змінною просторовою конфігурацією /

В.А. Дружинін, В.С. Наконечний, С.В. Толюпа, та ін. – К.: Логос, 2014. - 251 с.
[10] Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер. - М. Радио и связь. - 2000. - 519 с.
[11] Volodymyr Saiko, Serhii Toliupa, Volodymyr Nakonechnyi, Serhii Dakov (2018). The Method For Reducing Probability of Incorrect Data Reception In Radio Channels of Terahertz Frequency Range. 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET-2018, 174.
[12] Малыгин В.И. Один из способов защиты широкополосных систем связи от мощных узкополосных помех / В.И. Малыгин // Телекоммуникации. - 2001. - №11. - С. 18-22.
[13] Баруздин С.А. Нелинейная фильтрация узкополосных помех на основе ядерного магнитного резонанса / С.А. Баруздин // Радиотехника. - 2001. - №5. - С. 12.
[14] Yudin O. K. et al. Basic Concepts and Mathematical Aspects in Channel Coding: Multialternative Rules //Cybernetics and Systems Analysis. – 2016. – Т. 52. – №. 6. – С. 878-883.
[15] Yudin O. K. et al. A Method for Determining Informative Components on the Basis of Construction of a Sequence of Decision Rules //Cybernetics and Systems Analysis. – 2016. – Т. 52. – №. 2. – С. 323.
[16] Наконечний В.С. Задачі аналізу електромагнітної сумісності радіотехнічних засобів в сучасних інформаційно-вимірювальних системах / В.А. Дружинин, В.С. Наконечний, С.В.Толюпа // Науково-технічний журнал "Сучасний захист інформації". – 2014. – № 2. – С. 89–95.
[17] Наконечний В.С. Огляд сучасних радіоелектронних пристроїв на основі штучних магнітодіелектриків і метаматеріалів / В.С. Наконечний // Зв'язок. – 2014. -№4. – С. 48–56.
[18] Мельникова Л.И. Методы обеспечения электромагнитной совместимости в коллективе радиоэлектронных средств связи на этапе функционирования / Л.И. Мельникова // Восточно-европейский журнал передовых технологий. - 2004.- №4(10). - С. 80-83.
[19] Седельников Ю.Е. Электромагнитная совместимость радиоэлектрон-ных средств: учеб. пособ. / Ю.Е. Седельников. - Казань.: ЗАО «Новое знание», 2006. - 304 с.
[20] Малков, Н.А. Электромагнитная совместимость радиоэлектронных средств :учеб. пособие / Н.А. Малков, А.П Пудовкин. - Тамбов : Изд-во Тамб.гос. техн. ун-та, 2007.- 88 с.

Лукова-Чуйко Наталія Вікторівна
Доктор технічних наук , доцент, доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Інтереси: інформаційні технології, криптографія, інформаційна та кібербезпека.
Наука: автор більше 60 наукових праць.

Наконечний Володимир Сергійович
Доктор технічних наук, старший науковий співробітник, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Інтереси: системи розпізнавання багатопозиційного базування, системи технічного захисту інформації, кібербезпека та кіберзахист.
Наука: автор більше 130 наукових праць.

Сайко Володимир Григорович
Доктор технічних наук, професор, професор кафедри прикладних інформаційних систем Київського національного університету імені Тараса Шевченка.
Інтереси: радіоінженерія, інформаційні технології.
Наука: автор більше 270 наукових праць, 4 монографій, 25 патентів на винахід.

Толюпа Сергій Васильович
Доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Інтереси: інтелектуальні системи управління, напрямки підвищення ефективності функціонування інформаційних технологій, системи технічного захисту інформації, кібербезпека та кіберзахист..
Наука: автор більше 160 наукових праць.

DOI: https://doi.org/10.17721/ISTS.2019.1.79-87
УДК 005.8:316.422

ДОСЛІДЖЕННЯ МЕТОДІВ ПРОАКТИВНОГО УПРАВЛІННЯ ВІДХИЛЕННЯМИ НА ОСНОВІ НЕЙРОМЕРЕЖ В ІТ ПРОЕКТАХ

Морозов Віктор [1]
orcid.org/0000-0001-7946-0832

Кальніченко Олена [2]
orcid.org/0000-0002-8003-6980

Мезенцева Ольга [3]
orcid.org/0000-0002-8430-4022

Київський національний університет імені Тараса Шевченко, м. Київ
[1] knumvv@gmail.com, [2] kv_vl@ukr.net, [3] olga.mezentseva.fit@gmail.com

Історія статті:
Надійшла до редакції 25.06.2019
Прийнято 05.08.2019

Ключові слова:
хмарні технології;
розподілені інформаційні системи;
ІТ-проекти;
управління проектами;
проактивне управління;
інформаційні впливи;
взаємодія;
управління змінами.

Анотація: У даній роботі міститься опис результатів дослідження запропонованих методів проактивного управління відхиленнями ключових параметрів в складних проектах на основі дослідження впливів зовнішнього та внутрішнього оточення таких проектів. Запропоновано методи прогнозування рівня змін в результатах проектної діяльності в будь який час при виконанні проектів і в залежності від змін часових параметрів робіт проектів та дослідження впливів на зміни вартостей робіт проектів. Досліджуються реакції впливів на параметри вартості та часові параметри проектів. Розроблена інтегрована інформаційна система для моделювання потоків змін ключових параметрів ІТ-проектів з використанням хмарних сховищ даних. В процесі моделювання задіяні та інтегровані сучасні інформаційні технології управління проектами провідних розробників. В якості інструментів дослідження використовується моделювання впливів оточення на параметри проектів на основі моделей нейронних мереж глибинного навчання. Запропонована модель поглибленого навчання нейромережі, за рахунок експериментального представлення вхідних та вихідних даних чисельних експериментів. Така модель враховує оптимістичний та песимістичний розподіл вартості кожного з проектів під час планування проектів та вибору їх оптимальної конфігурації. Оцінка результатів моделювання впливів змін на терміни та вартість виконання робіт здійснюється з урахуванням контекстних характеристик проектів, серед яких розподіли ресурсів як у часі так і по роботам проектів, розподіли вартості тощо. Таким чином, змодельовані в системі показники вказують на незначні відхилення в межах 10–15% від заданих значень під впливом широкого діапазону значень факторів зовнішнього середовища і їх впливів на зміни обсягів ресурсів робіт проекту для обраної та незмінної технологічної конфігурації моделі проекту. Використовуючи проактивні засоби управління, при повторному моделюванні, стало можливим значно зменшити відхилення у витратах, які не перевищують 10% відхилення від оптимальних значень.

Abstract: This paper describes the results of a study of proposed methods of proactively managing key parameter deviations in complex projects based on the study of the effects of the external and internal environment of such projects. The methods of forecasting the level of changes in the results of project activity at any time during the execution of projects and depending on changes in the time parameters of the work of the projects and the study of the effects on changes in the cost of the work of the projects are proposed. Impact reactions on cost parameters and project timelines are investigated. An integrated information system has been developed to simulate the flow of changes to key IT project parameters using cloud data warehouses. In the process of modeling modern information technologies of project management of leading developers are involved and integrated. Modeling effects of the environment on project parameters based on models of deep learning neural networks are used as research tools. A model of deep learning of the neural network is proposed,

through the experimental representation of the input and output data of numerical experiments. This model takes into account the optimistic and pessimistic distribution of the cost of each project when planning the projects and choosing their optimal configuration. The evaluation of the results of modeling the effects of changes on the timing and cost of performing work is based on the context of project characteristics, including resource allocations both in time and in project work, cost allocations, etc. Thus, the modeled indicators in the system indicate slight deviations within 10-15% of the set values under the influence of a wide range of values of environmental factors and their effects on changes in project work resources for the selected and unchanged technological configuration of the project model. Using proactive controls, in the re-simulation, it became possible to significantly reduce deviations in costs that do not exceed 10% of the deviation from the optimum values.

1. ВСТУП

Стрімкий розвиток технологій в IT сфері обумовлений розвитком суспільства та збільшенням темпів життя. Сьогодні IT технології спрямовані на вирішення надскладних задач та задоволення потреб людства, наприклад, медицина, генетика, археологія, аерокосмічна галузь, тощо. При цьому спостерігається збільшення кількості новітніх розробок та створення більш складних та потужних розподілених інформаційних систем (РІС). Цьому сприяє швидкий розвиток хмарних обчислень, наприклад периферійні обчислення (edge computing), що створює нові можливості для обслуговування у хмарі [1], а також штучний інтелект, блокчейн, аналітика великих обсягів даних, квантові обчислювальні системи, тощо.

Зростаюча конкуренція, підвищення турбулентності процесів, які відбуваються в зовнішньому середовищі, збільшення складних непрогнозованих викликів призводять до необхідності переходу на «супергнучки застосунки» — контейнерні, безсерверні обчислення і інші технології, до характеристик яких відносяться модульність, розподіленість, постійна оновлюваність та використання хмарних обчислень [2, 3].

Створення складних гібридних систем, здатних задовольняти сучасні потреби, передбачає достатньо високу конструктивну та технологічну складність процесів розробки таких розподілених інформаційних систем. Для рішення зазначених надскладних задач доцільно використання проектного підходу [4, 5], який застосовує методи та інформаційні технології управління проектами. За останні 20 років використання таких засобів довели свою ефективність.

Застосування таких інформаційних технологій для управління IT-проектами, а також використання методів штучного інтелекту матиме значний вплив на ефективність результатів самих проектів.

Підтримку процесів розвитку сучасних методологій управління складними проектами проводили ряд українських вчених, професорів, зокрема Бушуєв С.Д. [6], Бушуєва Н.С. [7], Гогунський В.Д. [8], Морозов В.В. [9], Тесля Ю.М. [10], Білощицький А.О. [11] та інші. Зокрема, глибоко вивчено сферу управління проектами, дії змін, а також питання синтезу конфігурації проектного продукту в різних предметних областях, зокрема в розподілених проектах. Проте, проблема вибору оптимального набору контрольованих елементів проекту, на які впливають зміни, не була глибоко досліджена, щоб запропонувати свої практичні рішення, у тому числі в проектах розробки та впровадження РІС.

Постановка проблеми. У наведених роботах була частково формалізовані моделі елементів проектів, зокрема створення РІС у розподілених проектах. Однак фактори впливів IT-середовища [12] вимагають для таких складних проектів подальшого розвитку щодо визначення реакцій системи управління на зміни ключових параметрів проекту і побудови математичної моделі для проведення експериментальних досліджень.

Формулювання мети. Метою цієї роботи є розробка та дослідження методів прогнозування реакції системи управління проектами на основі моделювання нейромереж з глибинним навчанням при змінах параметрів основних характеристик проектів. Такі зміни з’являються в результаті дії інформаційних впливів зовнішнього оточення проекту.

Задачами дослідження є:

- аналіз поведінки системи під впливами зовнішнього оточення, що породжують різного роду зміни;
- проведення експериментального моделювання змін в реалізації складних IT-проектів;
- створення та дослідження варіантів розподілу ресурсів та часових параметрів

проектів для скорочення дій впливів на результати проектної діяльності.

Технічна та технологічна складність проектів розробки та інтеграції розподілених інформаційних систем полягає в необхідності вирішення багатокритеріальних задач, в забезпеченні широкого спектру функціональності та у використанні декількох технологій, що створює багаторівневу архітектуру таких систем. Крім того, на складність зазначених проектів також впливають фактори середовища, в якому проекти виконуються. Як було зазначено раніше, зовнішнє середовище проекту має *нестабільний та слабо прогнозований характер*.

При цьому, першочерговим завданням для управління проектами при розробці та впровадженні сучасних інтегрованих програмних застосунків з інтелектуальною підтримкою є оптимізація витрат [13 -15] на такі розробки та інтеграцію, а також оптимізація (скорочення) часу на їх розробку. Скорочення часу на розробку нового ІТ-продукту часто в сучасних ринкових умовах набуває найвищого пріоритету.

Тому пошук оптимальних варіантів розподілу ресурсів в ІТ-проектах може стати важливою задачею, успішне рішення якої забезпечить скорочення термінів виконання окремих проектних завдань та, як наслідок, всього проекту, крім того це може зменшити вартість проекту. При цьому прогнозування стану [16] таких проектів є багатовимірною задачею, яка може бути вирішена з використанням технологій сучасних нейронних мереж [17-21]. Крім того, слід враховувати значну кількість змін, які з'являються на різних етапах реалізації проекту та значно впливають на результати його виконання.

Таким чином, розгляд можливостей експериментального використання нейромереж в дослідженнях взаємодії чисельних змін на параметри ІТ-проектів з визначенням їх оптимальних станів є актуальним завданням.

2. ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ

Події, що відбуваються в проекті та події, що впливають на проект ззовні, визначають його глобальний стан в кожний момент часу. Цільовою функцією є збереження оптимального стану проекту протягом його реалізації. *Оптимальним станом* будемо називати стан, при якому спостерігається мінімізація дисбалансу елементів проекту, максимізація показника значущості цінностей проекту, як критерію досягнення поставлених цілей, і мінімізація шкоди (відхилень) від впливів зовнішнього оточення.

Оптимальний стан може бути досягнуто за рахунок активізації процесів проактивного управління. Це дозволить перейти від реагування на події до формування середовища максимально придатного для функціонування системи «проект-продукт-організація» («project-product-organization» P2O) [22] .

У якості початкового набору даних X, будемо використовувати опис задач проекту. При цьому вхідні параметри моделі проекту можна також представити у вигляді:

$$X(t)=\{x_1(t),x_2(t),...,x_i(t),...,x_n(t)\}, \quad (1)$$

при

$$x_i(t)=\left\langle ID_i, NM_i, \overline{T_i}, \overline{Rs_i}, \overline{Rl_i}, \overline{Cr_i}, C_i, Kr\right\rangle,$$

де $x_i(t)$ – опис стану k-ї задачі проекту на момент часу t, при $i=\overline{1,n}$ та $\forall t\in T$, ID_i – код ідентифікації задачі в проекті, NM_i – текстовий опис задачі або її назва, $\overline{T_i}$ – вектор часових параметрів поточної задачі проекту, $\overline{Rs_i}$ – вектор ресурсів передбачених для виконання задачі, $\overline{Rl_i}$ – вектор технологічних залежностей поточної задачі з іншими задачами, $\overline{Cr_i}$ – вектор вартісних характеристик ресурсних параметрів задачі, C_i – параметр вартості задачі, Kr – показник приналежності роботи до критичної задачі, T – час виконання проекту, n – кількість задач (робіт) проекту.

Оскільки для виконання проекту потрібно мати певну кількість ресурсів, то для проекту необхідно задати перелік таких ресурсів у вигляді певної множини R. Таким чином маємо:

$$R=\left\{r_i \mid j=\overline{1,m}\right\}, \quad (2)$$

де m – кількість трудових ресурсів, наданих для виконання даного проекту.

При цьому кожне r_j складається з:

$$r_j=\left\langle IR, NR, CR, MR, OR\right\rangle, \quad (3)$$

де IR – ідентифікатор певного ресурсу, NR – назва ресурсу, CR – цінова характеристика ресурсу (розцінка), MR – максимальна можлива завантаженість ресурсу, OR – характеристика виду ресурсу.

Як було викладено вище маємо тепер завантажити ресурси R^l для кожної задачі $x_i(t)$

проекту. При цьому отримаємо наступну матрицю:

$$R^l = \begin{pmatrix} r^l_{1,1} & \cdots & r^l_{1,m} \\ \vdots & \ddots & \vdots \\ r^l_{n,1} & \cdots & r^l_{n,m} \end{pmatrix}, \quad (4)$$

де $r^l_{i,j}$ – призначений обсяг l для j-го ресурсу і для i-ї роботи.

Визначене завантаження відбувається експертним методом. Однак, як зазначено в [23], основним підходом для отримання оцінок часу виконання робіт проекту є метод PERT (Program Evaluation and Review Technique). Він заснований на припущенні про бета-розподіл випадкової величини, що визначає тривалість виконання задач проекту. Тому, проводячи відповідні розрахунки за вказаним методом і використовуючи при цьому функцію β отримаємо розподіл ресурсів R^d на кожен період часу виконання проекту:

$$R^d = \xrightarrow{\beta(X)} = \begin{pmatrix} r^d_{1,1} & \cdots & r^d_{1,t} \\ & & \\ r^d_{n,1} & \cdots & r^d_{n,t} \end{pmatrix}, \; при\, t \in T \quad (5)$$

де $r^d_{n,t}$ – призначений обсяг ресурсів для i-ї роботи в період часу t.

Отримавши розподіл ресурсів у часі і знаючи їх розцінки CR_j, можна застосувати функцію μ визначення розподілу вартості проекту для кожної задачі проекту у часі.

$$C^d = \xrightarrow{\mu(\beta(X))} = \begin{pmatrix} c^d_{1,1} & \cdots & c^d_{1,t} \\ & & \\ c^d_{m,1} & \cdots & c^d_{m,t} \end{pmatrix} \quad (6)$$

Тоді запланована вартість проекту буде мати вигляд:

$$C_p = \sum_{i=1}^{n} \sum_{t=1}^{T} c^d_{i,t} \quad (7)$$

Розглянемо два варіанти змін, які найбільш характерні для будь-якого проекту.

1. Виходячи з умов експерименту щодо використання нейромережі та проведення її навчання нам треба отримати кілька спроб, які в процесі моделювання дадуть нам відповідні розподіли C^d_k, де $k \in K$ – кількість спроб моделювання (кількість матриць C^d). При цьому змінними, які ми будемо використовувати для моделювання, будуть саме варіанти R^l. Такі варіанти в даному випадку будуть вважатися за певний вид змін, які відбуваються під впливом зовнішнього оточення

Таким чином, на виході системи маємо сімейство кривих варіантів розподілу вартості проекту у часі. При цьому усереднений розподіл можна бути вважати за оптимальний:

$$C^a = \sum_{i=1}^{n} \sum_{t=1}^{T} \frac{\max(c^d_{i,t}) - \min(c^d_{i,t})}{2} \quad (8)$$

Відповідно отримаємо усередненій розподіл:

$$C^a = \xrightarrow{avar} = \begin{bmatrix} c^a_{1,1} & \cdots & c^a_{t,1} \\ \vdots & \ddots & \vdots \\ c^a_{1,m} & \cdots & c^a_{t,m} \end{bmatrix} \quad (9)$$

Завдяки навченої нейромережі можна отримати для знайденого оптимального графіку вартості проекту відповідне оптимальне завантаження ресурсів R^{la} для кожної з робіт проекту.

У подальшому, при використання проактивного управління IT проектами, для кожного з можливих варіантів R^l (які імітують зміни) будемо мати за допомогою розробленої моделі нейромережі різні варіанти відхилень прогнозованої вартості проекту $\pm\Delta C$ від оптимального варіанту.

2. Аналізуючи розподіл (4) необхідно звернути увагу на відповідність значень отриманих обсягів ресурсів в кожний момент часу t значенню MR (максимальна можлива завантаженість ресурсу) для даного ресурсу. У випадку, коли спостерігається перевищення ліміту ресурсу необхідно провести певну оптимізацію. Наприклад, ресурс $r^d_{1,1}$ працює понад 40 годин в перший тиждень реалізації проекту. Це свідчить про його перевантаження та передбачає необхідність вирішення даної проблеми шляхом збільшення тривалості роботи/робіт, які використовують даний ресурс в тиждень, що розглядається.

Після збільшення тривалості роботи/робіт, при незмінному обсягу ресурсу для даних роботи/робіт, отримуємо зменшення використання ресурсу у період часу, що розглядається. Іншими словами, при пропорційному завантаженні ресурсу його обсяг рівномірно розподіляється на більший період часу.

Крім того кожна робота має певну тривалість та ми можемо задати множину часових параметрів T^D (тривалостей) всіх робіт проекту:

$$T^D = \left\{ t^D_i \mid i = \overline{1,n} \right\} \quad (6)$$

При цьому вектор часових параметрів $\overline{T_i}$ роботи $x_i(t)$ може бути представлений кортежом параметрів:

$$\overline{T_i} = \left\langle T^D, T^S, T^F \right\rangle, \qquad (7)$$

де T_i^D – тривалість роботи;

T_i^S – час початку роботи;

T_i^F – час завершення роботи.

Після збільшення тривалості роботи/робіт, які містять перевантажені ресурси отримуємо матрицю скорегованого розподілу ресурсів, де окремі $r_{i,j}^d$ набули нові значення:

$$\grave{R}^d = \xrightarrow{\beta(X)} = \begin{pmatrix} r_{1,1}^d & \cdots & r_{1,t}^d \\ & & \\ r_{n,1}^d & \cdots & r_{n,t}^d \end{pmatrix}, \qquad (8)$$

Наступним кроком буде спроба переглянути тривалість проекту за рахунок зменшення тривалості окремих робіт з обов'язковою перевіркою на перевищення максимально допустимих значень MR для кожного ресурсу. Таких ітерацій може бути безліч доти, доки ми не отримуємо оптимальну тривалість проекту та при цьому позбавимось усіх перевантажень ресурсів:

$$T^D \xrightarrow{r_{i,j}^d \le R_j^{MR}} \min \mathrm{T}^D \qquad (9)$$

де $k \in K$ – кількість спроб моделювання (кількість матриць $\grave{R}^d$).

Виходячи з умов експерименту щодо використання нейромережі та проведення її навчання нам треба отримати кілька спроб, які в процесі моделювання дадуть нам відповідні розподіли C_k^d, де $k \in K$ – кількість спроб моделювання (кількість матриць C^d). При цьому змінними, які ми будемо використовувати для моделювання, будуть саме варіанти $\grave{R}^d$. Такі варіанти в даному випадку будуть вважатися за певний вид змін, які мають відбуваються під певним впливом зовнішнього оточення складних проектів. Як вже повідомлялося такі впливи мають турбулентний та слабко прогнозований характер.

Значення обсягів призначених на роботу ресурсів та вартість проекту не змінюється, а змінюється лише значення тривалості робіт проекту.

Завдяки навченої таким чином нейромережі можна отримати оптимальне завантаження ресурсів для кожної з робіт проекту. Тобто обрати з сімейства кривих розподілу вартості ту, що відповідає мінімально допустимому варіанту за часом.

У подальшому, при використання проактивного управління ІТ проектами, для кожного з можливих варіантів R^d (які імітують зміни) будемо мати за допомогою розробленої моделі нейромережі різні варіанти відхилень прогнозованої тривалості проекту $\pm\Delta T$ від оптимального варіанту.

3. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

Переходячи до етапу навчання нейронної мережі далі визначаємося з чисельними варіантами схем завантаження ресурсів по задачам проекту та бюджетними обсягами таких ресурсів, які в цьому підході задаються на весь період виконання задачі. Приклад одного з варіантів можливого завантаження показано в таблиці 1. Таких варіантів треба від 10 до 50. Ці варіанти завантажень і будуть генератором змін в проекті, що досліджується.

Для навчання нейромережі також необхідні для кожного варіанту завантаження задач (робіт) ресурсами мати на виході диференційований та кумулятивний (зростаючим підсумком) розподіл задіяних ресурсів у часі. Для отримання таких результатів скористаємося моделюванням в стандартних програмах з планування та моніторингу проектів, наприклад програмним забезпеченням компанії Oracle's Primavera [24], приклад використання якого показано на рис. 1. При цьому на графіку видно фрагмент переліку задач проекту, їх результат моделювання та розрахунку у часі, завантаженість певними видами ресурсів та сумарна вартість робіт.

Таблиця 1. Фрагмент схеми завантаження ресурсів певного виду на задачі проекту

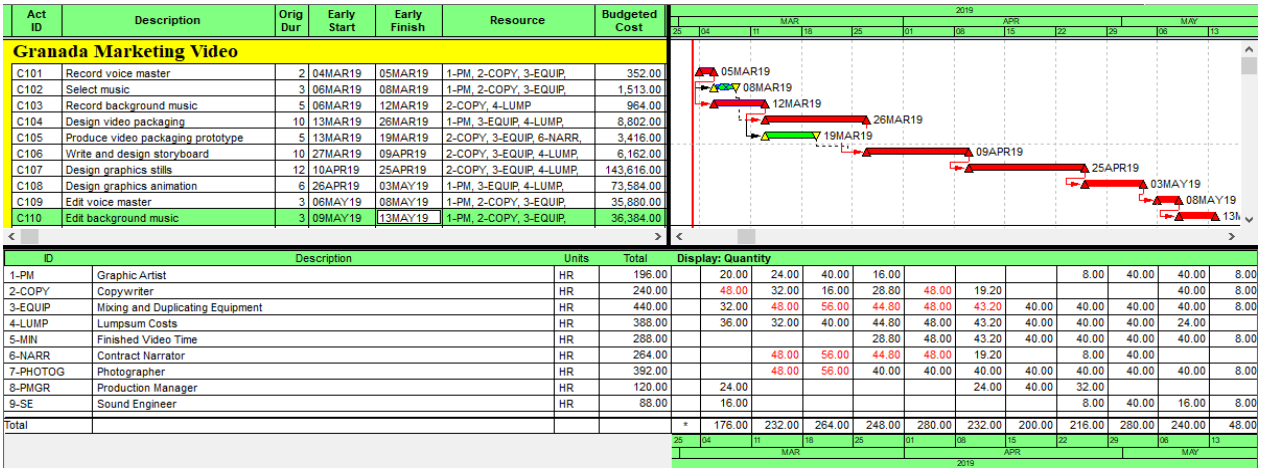
№ задачі	Номера та розподіл обсягів ресурсів									
	1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	..
1	4	6	4							..
2	1		8	8				1		..
3		4		4						..
4	1		2	2		4	2			..
5						4	8			..
6			2	2	4	2				..
7		2	3	4	2		2	1		..
8	1		2	2	2	2	2		1	..
9	1	1	2	2	4		1			..
10	1	1	1		1		1		4	
…	…	…	…	…	…	…	…	…	…	..

В нижній частині показані види ресурсів та їх необхідні сумарні обсяги на кожний період часу на протязі виконання усього проекту

Таким чином, для кожного варіанту завантаження задач ресурсами отримаємо два відповідних розподіли, варіанти яких показано на рис. 2 та рис. 3.

При цьому диференційований розподіл покаже нам пікові навантаження або провали в обсягах використання ресурсів (рис. 2). Кумулятивна діаграма покаже, який з ресурсів у часі є найбільш завантаженим, а якій навпаки.

В результаті моделювання варіантів завантажень задач ресурсами для нашого проекту щодо визначення їх вартості отримаємо сімейство кривих, приклад яких наведено на рис.4.



Act ID	Description	Orig Dur	Early Start	Early Finish	Resource	Budgeted Cost
Granada Marketing Video						
C101	Record voice master	2	04MAR19	05MAR19	1-PM, 2-COPY, 3-EQUIP,	352.00
C102	Select music	3	06MAR19	08MAR19	1-PM, 2-COPY, 3-EQUIP,	1,513.00
C103	Record background music	5	06MAR19	12MAR19	2-COPY, 4-LUMP	964.00
C104	Design video packaging	10	13MAR19	26MAR19	1-PM, 3-EQUIP, 4-LUMP,	8,802.00
C105	Produce video packaging prototype	5	13MAR19	19MAR19	2-COPY, 3-EQUIP, 6-NARR,	3,416.00
C106	Write and design storyboard	10	27MAR19	09APR19	2-COPY, 3-EQUIP, 4-LUMP,	6,162.00
C107	Design graphics stills	12	10APR19	25APR19	2-COPY, 3-EQUIP, 4-LUMP,	143,616.00
C108	Design graphics animation	6	26APR19	03MAY19	1-PM, 3-EQUIP, 4-LUMP,	73,584.00
C109	Edit voice master	3	06MAY19	08MAY19	1-PM, 2-COPY, 3-EQUIP,	35,880.00
C110	Edit background music	3	09MAY19	13MAY19	1-PM, 2-COPY, 3-EQUIP,	36,384.00

ID	Description	Units	Total	Display: Quantity										
1-PM	Graphic Artist	HR	196.00		20.00	24.00	40.00	16.00				8.00	40.00	40.00	8.00
2-COPY	Copywriter	HR	240.00		48.00	32.00	16.00	28.80	48.00	19.20				40.00	8.00
3-EQUIP	Mixing and Duplicating Equipment	HR	440.00		32.00	48.00	56.00	44.80	48.00	43.20	40.00	40.00	40.00	40.00	8.00
4-LUMP	Lumpsum Costs	HR	388.00		36.00	32.00	40.00	44.80	48.00	43.20	40.00	40.00	40.00	24.00	
5-MIN	Finished Video Time	HR	288.00					28.80	48.00	43.20	40.00	40.00	40.00	40.00	8.00
6-NARR	Contract Narrator	HR	264.00			48.00	56.00	44.80	48.00	19.20		8.00	40.00		
7-PHOTOG	Photographer	HR	392.00			48.00	56.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	8.00
8-PMGR	Production Manager	HR	120.00		24.00					24.00	40.00	32.00			
9-SE	Sound Engineer	HR	88.00		16.00							8.00	40.00	16.00	8.00
Total				*	176.00	232.00	264.00	248.00	280.00	232.00	200.00	216.00	280.00	240.00	48.00

Рис. 1 – Приклад інтеграції процесів моделювання на основі програмного забезпечення з управління проектами та програмами для IT-проектів

Рис. 2 – Приклад варіанту розподілу і часі ресурсів проекту по тижнях

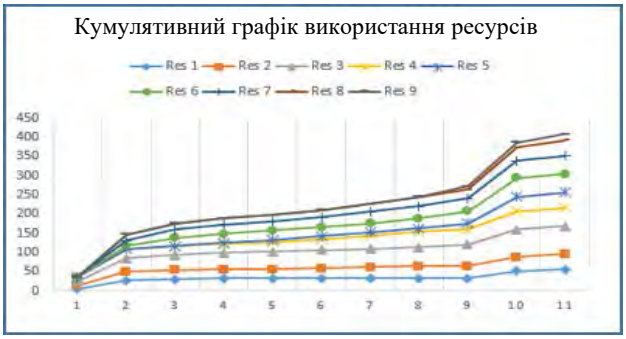


Рис. 3 – Розрахунок ресурсів зростаючим підсумком

Уся ці отримані дані також заносяться до нейромережі на етапі її навчання. Але, аналізуючи сімейство кривих вартості можна візуально та аналітично визначити максимальні та мінімальні розподіли. При чому, максимальний в даному випадку буде сформовано по двом (кільком) варіантам генерації завантажень задач ресурсами, так само як і мінімальний варіант.

На практиці, з комерційної точки зору, це свідчить про наявність можливого оптимістичного та песимістичного варіантів завершення будь-якого IT проекту.

Рис. 4 – Результати впливів змін на початкові реакції системи у вигляді розподілів вартості проекту

Але найбільш цікавим є усереднений розподіл вартості проекту в часі, що є на практиці компромісним варіантом між замовником проекту та його виконавцями. Приклади таких розподілів показані на рис. 5. Усереднений графік і є оптимальним результатом (виходом) нашої системи.

Для проведення експериментів та навчання нейромережі [25 - 27] використовувалося спеціально розроблена модель, фрагмент якої наведено на рис. 6.

Для другого варіанту, що розглядався як типові зміни в проекту, приклад завантаження задач ресурсами наведений в таблиці 2. Варіанти змін тривалості задач наведені у таблиці 3.

Рис. 5 – Визначення усереднених результатів розподілу вартості проекту

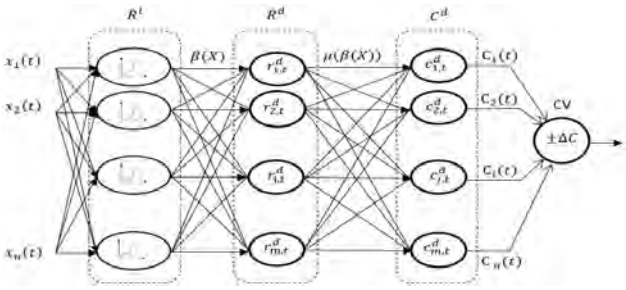


Рис. 6 – Архітектура ансамблю використовуваних нейронних мереж

Table 2. Фрагмент схеми завантаження задач обсягами ресурсів

Task ID	Resource ID								
	1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***
1	0,5		0,5			0,5	1/4		
2			1/4	1				0,5	0,5
3		1		0,5		1/4			
4	1/4		0,5			1	0,5		¼
5	0,5			0,5	1	0,5		1/4	¼
6			1/4	0,5	0,5	0,5	0,5		
7	1/4	1/4	0,5	1/4	0,5			1/4	
8	1/4			0,5		1	1/4	1	0,5
9		0,75	1/4		0,6		¼	1/4	
10	1/4	0,5	1/4		0,5		0,5	1	1

Після завантаження задач ресурсами отримаємо два відповідних розподіли, варіанти яких показано на рис. 7 та рис. 8. При цьому диференційований розподіл покаже нам пікові навантаження або провали в обсягах використання ресурсів (рис. 7). Кумулятивна діаграма покаже, який з ресурсів у часі є найбільш завантаженим, а якій навпаки.

Table 3. Фрагмент розподілу варіантів змін часових характеристик робіт

Task ID	Варіанти розподілу часових характеристик параметрів робіт проекту						
	1	***2***	***3***	***4***	***5***	...	***50***
1	3	4	3	3	2	...	3
2	6	7	7	7	7	...	8
3	8	11	10	10	9	...	9
4	13	15	14	13	13	...	12
5	5	5	5	5	5	...	4
6	15	15	15	15	13	...	14
7	12	13	13	13	13	...	11
8	10	11	11	10	10	...	8
9	3	6	6	6	6	...	5
10	3	4	4	3	3	...	3

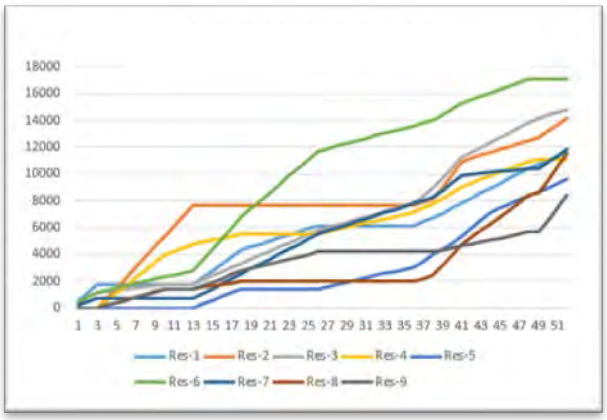


Рис. 7 – Розподіл ресурсів в часі при зміні часових параметрів задач

В результаті моделювання варіантів тривалостей задач для нашого проекту отримуємо сімейство кривих розподілу ресурсів в часі у вартісному вираженні, приклад яких наведено на рис. 8.

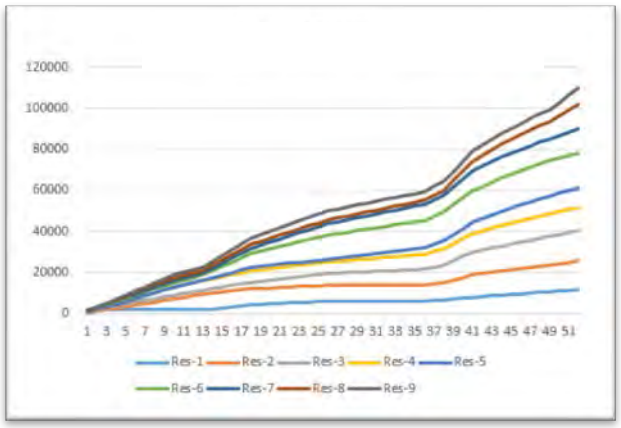


Рис. 8 – Розподіл ресурсів зростаючим підсумком при зміні часових параметрів задач проекту

Усі ці отримані дані також заносяться до нейромережі на етапі її навчання. Аналізуючи сімейство кривих вартості можна візуально та аналітично визначити максимальні та мінімальні

розподіли за часом при однакових значення вартості проекту.

Залишається питання визначення оптимальних тривалостей задач для отримання мінімального за часом графіку вартості. Рішення можна отримати чисельними розрахунками, поступово наближаючись до заданого вихідного результату.

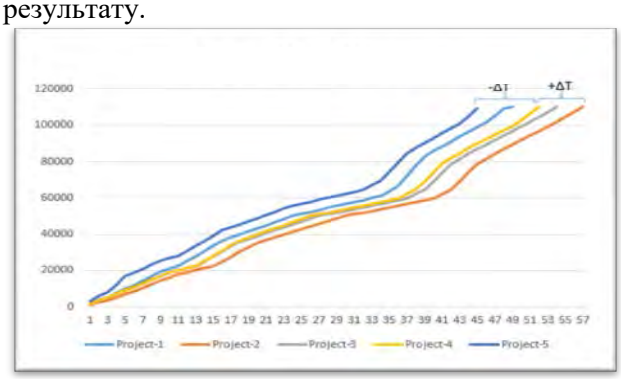


Рис. 9 – Результати змін початкових реакцій системи у вигляді варіантів вартості

Але це займе дуже багато часу і буде достатньою дорогим процесом. Тому використання нейромереж є ефективним рішенням для вирішення подібних задач.

4. РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ

В наведених дослідженнях було розглянуто два варіанти змін:

- зміни схем завантаження робіт ресурсами, обсягів ресурсів при незмінних параметрах тривалості робіт
- зміни часових параметрів робіт при сталих обсягах та схемах завантаження ресурсів на роботи.

Активаційні функції при цьому обиралися з лінійної, квадратичної, кубічної, сігмоїдальної функцій. Через те, що час роботи програми значно збільшується в результаті такого перебору, реалізованого у прихованому циклі. Ми зупинилися на використанні сигмоїдальної функції активації у прихованому і вихідному шарах нейронної мережі.

Оцінюючи результати експериментів можна провести оцінку і зробити певні висновки. Зокрема було з'ясовано, що при достатньо широкому діапазоні змін вхідних параметрів моделі на виході ми отримували незначні коливання змін реакцій системи ($\pm\Delta C$). Це характерно лише для даної конфігурації сітьової моделі (технології створення продукту проекту), часових параметрів робіт проекту, обмежень тощо.

При фіксації обсягів робіт та серії змін для часових параметрів робіт моделі проекту отримуємо криві розподілу вартості, які відхиляються в меншу та в більшу сторону значень від оптимального значення за умовою мінімально допустимої тривалості проекту.

5. ВИСНОВКИ

1. Запропоновані методи проактивного управління відхиленнями по часу та вартості проектів з використанням нейромереж з глибинним навчанням для аналізу змін в реакціях системи управління складними IT-проектами на основі впливи зовнішнього турбулентного оточення показали свою ефективність. Відмінною особливістю такого підходу є цілісне уявлення і аналіз впливу середовища на множину всіх елементів проекту з сильними взаємодіючими відносинами та впливами.

2. Наведена математична модель процесів глибинного навчання штучних нейромереж дозволила формалізувати процеси реалізації проектів на основі проактивного підходу та визначити цільові функції для подальшого дослідження поведінки моделі під впливом турбулентного середовища. Вартість та час реалізації проекту були взяті за основу, як основні параметри, що визначають ефективність проекту.

7. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] *Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X08001957.

[2] B. Furht, A. Escalante, *Handbook of Cloud Computing*, https://link.springer.com/book/10.1007/978-1-4419-6524-0.

[3] А. Алпатов, "Развитие распределенных технологий и систем", *Перспективы науки и образования*, 2015, вып. 2 (14).

[4] A. Kintonova, Z. Bakkaisha, A. Madina and E. Maikibaevaa, "Development of Distributed System for Electronic Business Based on Java-Technologies". *International journal of environmental & science education,* Vol. 11, №. 10, p. 3861-3883, 2016.

[5] N. Bessis, "Development of Distributed Systems from Design to Application and Maintenance". *Edge Hill University*, UK, 2013.

[6] С. Бушуєв, М. Дорош, "Формування інноваційних методів та моделей управління проектами на основі конвергенції". *Управління розвитком складних систем*, №23, С. 30-37, 2015.

[7] Н. Бушуєва, *Моделі та методи проактивного управління програмами організаційного розвитку*, [Посібник], К.: Науковий світ, 2007, 199 с.

[8] V. Gogunskiy, K. Kolesnikova, D. Lukianov, "Lifelong learning is a new paradigm of personnel training in enterprises", *Eastern-European Journal of Enterprise Technologies.* № 4/2 (82). pp. 4–10, 2016.

[9] V. Morozov, O. Kalnichenko, I. Liubyma. „Proactive Project Management for Development of Distributed

Information Systems". *Proceedings of the 4th International Scientific and Practical Conference "Problems of Infocommunications. Science and Technology" (PIC S&T-2017)*, Kharkiv, Ukraine, 2017.

[10] Yu. Teslia, A. Khlevnyi, I. Khlevna. "Control of informational Impacts on project management". *Proceedings of the 1th IEEE International Conference on Data Stream Mining & Processing*, 23-27 August. Lviv, Ukraine, 2016.

[11] A. Biloshchytskyi, A. Kuchansky, Yu. Andrashko, S. Biloshchytska, O. Kuzka, Ye. Shabala, T. Lyashchenko, "A method for the identification of scientists' research areas based on a cluster analysis of scientific publications". *Eastern-European Journal of Enterprise Technologies, 5*. – Vol. 2. – Issue 89. 4-10, 2017.

[12] *Проактивное управление проектами*, [Online]. Available: http://www. itexpert.ru/rus/ITEMS/ 200810062247/.

[13] P. Kenneth "Birman: Reliable Distributed Systems: Technologies", *Web Services, and Application,* 2005

[14] O. Maimon, L. Rokach, "Data Mining and Knowledge Discovery Handbook", 2005, [Online]. Available: http://www.bookmetrix. com/detail/book/ae1ad394-f821-4df2-9cc4-cbf8b93edf40.

[15] М.С. Косяков, *Вступ до розподілених обчислень*, СПб: Інститут державних досліджень IST, 2014, 155 с.

[16] *A Guide to the Project Management Body of Knowledge (PMBOK®). Sixth Edition*. – Delaware, Pennsylvania, Newton Square 19073-3299, USA: Project Management Institute Four Campus Boulevard, 2017, 586 p.

[17] S. Warrilow. *Change management: the horror of it all, Project Smart.* 2010. [Online]. Available: https://www.projectsmart.co.uk/change-management-the-horror-of-it-all.php.

[18] W. Carsten, "Multi-agent System of IT Project Planning", *Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Vol. 1, 21-23 September, Bucharest*, 2017, pp. 548-553.

[19] Leticia Fuentes Ardeo, Maria Aguilar, Jose Ramon Otegi Olaso. "The Project Knowledge Management: a key factor in the integration of Sustainability in Project Management", *Proceedings of International Research Conference at the Dortmund University of Applied Sciences and Arts,* Dortmund, Germany, 30 June - 1 July, 2017, pp. 96-98.

[20] Дж. Гараедаги. *Системное мышление. Как управлять хаосом и сложными процессами. Платформа для моделирования архитектуры бизнеса*, Минск: Гревцов Букс, 2010, 480 с.

[21] E. Murray, I. Zakharova. *Knowledge Management Success, Effectiveness Models*, [Online]. Available: http://www.management.com.ua/strategy/str113.html

[22] V. Morozov, O. Kalnichenko, S. Bronin, "Development Of The Model Of The Proactive Approach in Creation Of Distributed Information Systems", *Eastern-European Journal of Enterprise Technologies,* № 43/2 (94), pp. 6-15, 2018.

[23] Ю. Ю. Самохвалов, "Розробка методу прогнозування графа в умовах неповноти та неточності експертних оцінок", *Журнал "Кібернетика і системний аналіз",* том. 54, №1, стор. 84-91, 2018.

[24] *Oracle's Primavera P6 Enterprise Project Portfolio Management,* [Online]. Available: https://www.oracle.com/applications/primavera/products/project-portfolio-management/, last accessed 2019/03/25.

[25] А. С. Новиков, А.А. Ежов, "Многослойная нейронная сеть Розенблатта и ее применение для решения задачи распознавания подписей", *Известия ТулГУ. Технические науки,* 2016, № 2. С. 188-197.

[26] В.И. Комашинский, Д.А. Смирнов Д.А., *Нейронные сети и их применение в системах управления и связи*, Горячая линия-Телеком, 2003, 94 с.

***Віктор Морозов**, к.т.н., професор, завідувач кафедри Технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченко, Україна. Він має досвід викладання та досліджень, керуючи складними проектами понад 30 років. Він є автором понад 200 статей у різних міжнародних журналах і виданнях відомих національних і міжнародних конференцій. Сучасні наукові інтереси включають проблеми складних дистрибутивних IT-проектів з використанням хмарних технологій. Член IEEE.*

***Олена Кальніченко,** кандидат технічних наук, доцент кафедри Технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Разом з викладацькою та дослідницькою діяльністю автор брав участь у проектах з впровадження корпоративних систем управління проектами та у створенні Офісів управління проектом в IT та будівельних компаніях. Сертифікований професійний менеджер проектів (IPMA).*

***Ольга Мезенцева,** кандидат економічних наук, асистент кафедри Технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. За успіхи у навчально-науковій діяльності автор отримав стипендію Верховної Ради України та стипендію Президента України. Автор більше 40 наукових публікацій у вітчизняних та зарубіжних виданнях, включених до міжнародних наукометричних баз даних. Основні напрями науково-дослідної діяльності: інформаційно-економічна аналітика, інструменти та впливи, системи управління інформаційними ризиками, інформаційні системи в бізнесі.*

DOI: https://doi.org/10.17721/ISTS.2019.1.66-78
УДК 621.39 (045)

ПІДВИЩЕННЯ НАДІЙНІСНИХ ПОКАЗНИКІВ ПРОГРАМНО-ОРІЄНТОВАНОЇ МЕРЕЖІ

Даков Сергій [1]
orcid.org/0000-0001-9413-3709

Дакова Лариса [2]
orcid.org/0000-0001-6104-8217

[1] Київський національний університет імені Тараса Шевченко, м. Київ
[2] Державний університет телекомунікацій, м. Київ

Історія статті:
Надійшла до редакції 23.06.2019
Прийнято 01.08.2019

Ключові слова:
програмно – конфігурована мережа;
мобільна мережа; ;
централізована мережа;
децентралізована мережа;
гетерогенна мережа
.

Анотація: *В роботі проаналізовані надійнісні показники програмно-орієнтованої мережі, зроблено порівняння централізованих та децентралізованих типів керування виявлено що програмно-керовані мережі потребують оптимізації та підвищення надійності до сучасних стандартів 3gpp. Запропонована модель розрахунку надійності централізованої та децентралізованої мереж, за допомогою якої можливо визначити слабкі або менш надінісні місця в системі мобільного зв'язку. Розроблено метод оцінювання та підвищення надійнісних характеристик інформаційно-управляючої системи мережі мобільного зв'язку, на базі ієрархічної моделі оцінки надійності апаратних та програмних засобів. Врахована залежність обладнання від програм або додатків. Система дозволяє оптимізувати процес розгортання мережі, модернізації та підвищити надійність обслуговування абонентів мобільних мереж. Що значно поліпшує процес планування та моделювання інфраструктури мережі, яка в свою чергу збільшує ефективність використання та зменшує витрати на обладнання і трудові затрати людино-годин. Також пропонується дану математичну модель використати для розробці програмного забезпечення та встановити на гіпервізрх у вигляді додатка на централізовані типи мереж, що допоможе підвищити ефективність використання інфраструктури, зменшити час реагування на відновлення працездатності систем мобільного зв'язку. Промодельовані три типи сучасних технологій керування інфраструктурою мобільних мереж а саме IP, OpenFlov та Overlay. Визначено що для мереж майбутнього більш доцільніше використовувати саме програмно-керовані мережі, які мають більш розвинену модель керування але менш надійні сну структуру, тому її оптимізація є необхідним фактором в використання саме цих типів мереж.*

Abstract: *In this work the reliable indicators of the software-oriented network were analyzed, the comparison of centralized and decentralized management types was made, that program-managed networks need to optimize and increase reliability to the current standards of 3gpp. The model of calculation of the reliability of centralized and decentralized networks is proposed, with the help of which it is possible to identify weak or less susceptible sites in the mobile communication system. The method of estimation and enhancement of reliable characteristics of the information management system of the mobile communication network is developed, based on the hierarchical model of hardware and software reliability assessment. The dependence of equipment on applications or applications is taken into account. The system allows to optimize the process of deployment of the network, modernization and increase the reliability of servicing subscribers of mobile networks. This significantly improves the planning and modeling of the network infrastructure, which in turn increases the efficiency of use and reduces the cost of equipment and labor costs of man-hours. It is also proposed to use this mathematical model for software* management model but less reliable sleep structure, so its optimization is a necessary factor in the use of these types of networks.

1. ВСТУП

Основна задача теорії надійності покращити показники системи за допомогою підвищення надійнісних характеристик об'єкту. За

допомогою прорахунку оптимального числа обслуговування системи для покращення її технічних показників

Об'єктом дослідження являєтеся мобільна мережа 3 GPP, яка на сьогоднішній час є самою актуальною Гетерогенна мережа або smoll – sell доповнює інфраструктуру сучасної мобільної мережі. Всі ці стандарти дуже поширюють спектр вразливості мереж як фізичної інфраструктури.

Метою роботи є підвищення надійністних показників комп'ютерної мережі.

Для досягнення поставленої мети необхідно вирішити наступні основні завдання:

Розробити метод оцінки надійнісних характеристик комп'ютерних мереж.

Розробити метод підвищення надійнісних характеристик комп'ютерних мереж.

Тому для подібні структури мережі треба, мати якусь статистику надійності, вразливості системи, не лише в кіберпросторі, але й фізичної інфраструктури.

Так як, за допомогою програмного забезпечення виходить з ладу фізичне обладнання. Тому треба розуміти де вразливі місця системи і мати це на увазі.А допомогти цю інформацію дослідити за допомогою математичних обгартувань процесу, показники якого будуть проаналізовані та прийняті на увазі.

Також за допомогою більш глибокого аналізу можна розробити математичну модель яка буде оброблювати статистику прораховати надійність кожного вибраного сегменту, який в свою чергу має особисту цифру всієї системи, показує залежність.

Для майбутнього розвитку системи проектування програм моніторингу любого об'єкту, в нашому випадку, це мережі 3,5G (HSPA +) 4G, 5G,тощо. Показники надійності цих стандартів повинні дорівнювати коефіцієнт надійності стандарту.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

В статті [1] автор акцентує увагу на складній системі керування мобільною інфраструктурою, яка складається з багатьох інструментів та можливостей програмно-керованої мережі, але зовсім не зосереджена увага невисокій надійності мережі SDN.

Аналіз літератури показав, що велику роль присвячено дослідженню питань надійності системи SDN, що цим самим показує рівень вразливості системи, наприклад в статті [2] запропоновано компенсувати низьку надійність перемиканням з мережі OpenFlow на класичну мережу, що саме допоможе підтримати працездатність мережі та підвищиться її надійність. Варто розуміти, технічні показники мережі значно знизяться, тому що IP мережа за поступається технічними показниками, що можна побачити в роботі [3] При переході на більш сучасну мережу можливо отримати на деяких ділянках перевантаження та зниження якості послуги, але треба підкреслити, що саме надійність OpenFlow дійсно набагато вище ніж у мережі Owerlay.

В статті [4] розглянуто метод роботи мережі в перевантаженому режимі, що в комплексі вирішує проблему переключення з SDN на IP, але низька надійність мережі Owerlay залишається, що робить в використанні мережу практично неможливою для оператора мобільної, або стаціонарної мережі великих об'єктів.

В моделях 3 GPP коли будується мережа аналізуєтеся її надійність, так як сфера використання, наприклад дистанційне керування об'єктами чи маніпуляторами [5, 6].

А для стандарту 4G та 5G надійність має певне значення і не може бути забезпечена контролером SDN та обладнання інших рівнів [6, 7].

Варто зазначити, що робота над надійністю мережі має дуже важливий характер та для централізованих мереж - це життєво важливий цикл, тому необхідно застосувати додаткові інструменти.

Зазначимо, що вартість централізованих мереж також має дуже велике значення, що відмічено в статті [8].

Багато проблем можна вирішити за допомогою програмного забезпечення, встановлюється на прикладний рівень програмно-керованої мережі або ПКМ [9].

За допомогою нього є можливість керувати процесами та автоматизувати багато процесів мережі, зокрема об'єднати існуючі моделі та функції. Саме в комплексі ці моделі зможуть зменшити вартість та підвищити показники мережі, вилучити саме ті недоліки, які не згадані в роботах на теми централізованих ПКМ.

Враховуючи вищезгадане треба зазначити, що ключові проблеми програмної мережі полягають у вартості та надійності системи, що мають менші показники ніж існуюча, класична мережа IP, яка за часом здобула і стандарти і промислове визнання

Уже сьогодні анонсують стандарт з більшими технічними характеристиками, але впровадити його за децентралізованою архітектурою майже неможливо, тому вирішення проблеми надійності має дуже важливий характер. Також проблема вартості інфраструктури робить

використання технології SDN нерентабельною, тому зменшення вартості інфраструктури – не менш важлива проблема цієї мережі.

Так як комп'ютерна мережа має динамічну структуру, то вирішити це можливо за допомогою програмного забезпечення для автоматизації функціональних завдань керування мережею, аналізу й оцінювання ефективності автоматизованих систем переробки інформації й управління.

Тому дана тема роботи є актуальною та має проблему сучасного характеру.

3. ПОСТАНОВКА ЗАВДАННЯ

Сучасні стандарти мобільних мереж повинні мати показники надійності на рівні 99.999% що робить процес розгортання мережі важким, так як усі розрахунки треба робити вже на етапі планування інфраструктури опорного сегменту. Треба враховати планування та модернізацію мережі.

Сьогоднішні моделі не мають показники означені стандартом, тому треба розглянути методи та моделі підвищення надійності комп'ютерної мережі за допомогою теорії надійності.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розрахунок надійності мережі SDN

Програмно-керована система має недоліки такі як велика вартість та низька надійність, що виходить самої архітектури клієнт – сервер або з її централізованого вигляду.

До того ж треба врахувати що основний тип промислових мереж має вигляд гетерогенної мережі але за допомогою SDN можливо поліпшати керування цієї мережі та підвищити динаміку впровадження нового обладнання яке може відрізнятися не лише такими критеріями як: пропускна здатність, затримка та повторне використання ресурсу, але різновидом інтерфейсу та адаптивними можливостями обладнання. Що дуже ускладняє роботу персоналу та робить можливість обслуговування мережі дуже важким та затратним.

Програмно орієнтована мережа – це і є основна технологія за допомогою якої можливо покращіти показники мобільної мережі а ле структура мережі клвєнт сервер як сказано віще, має ряд значних недоліків яки треба подолати щоб впровадити данну технологію на приомисловий рівень.

Перший й основний недолік – це надійність мережі, із за центру керування, контролеру, який керує мережею і як що він вийде з ладу мережа стає не робота - способна. Надійність мережі та інщі недоліки (наприклаж вартість інфраструктури), можливо вирішити за допомогою, побудови інформаційних технологій для автоматизації функціональних завдань керування, аналізу й оцінювання ефективності автоматизованих систем переробки інформації й управління.

Тому по перше треба визначити модель розрахунку мережі.

На рис. 1, 2, 3 зображена архітектура транспортних сигментімобільної мережі LTE

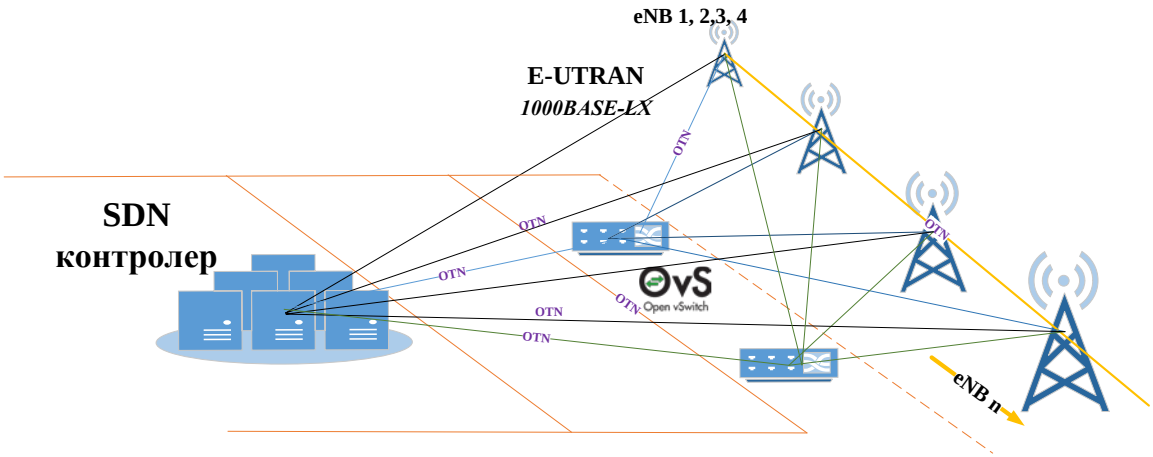


Рис.1 - Архітектура software-defined networking

Архітектура програмно орієнтованої мережі ієрархічно залежну, складну, багато підревневу систему передавання потоків трафіку за допомогою процесів керування контролером SDN, який керує OvS свічами, де знаходиться таблиця переадресації.

Недоліки такої архітектури в тому що працездатність кожного рівня залежіть від

іншого і тому з'єднання таких смуг не надійне, але ця мережа має більш ефективні показники тому основна задача підняти надійність та розробити модель розподілу, резервування та рознесення слабких частин системи.

а рис.5 зображена архітектура мобільної мережі, побудована на базі протоколу класичної IP технології адресації вузлів. Тут кожний елемент системи працює автономна, структура такої мережі вважається децентралізованою тому надійність більша.

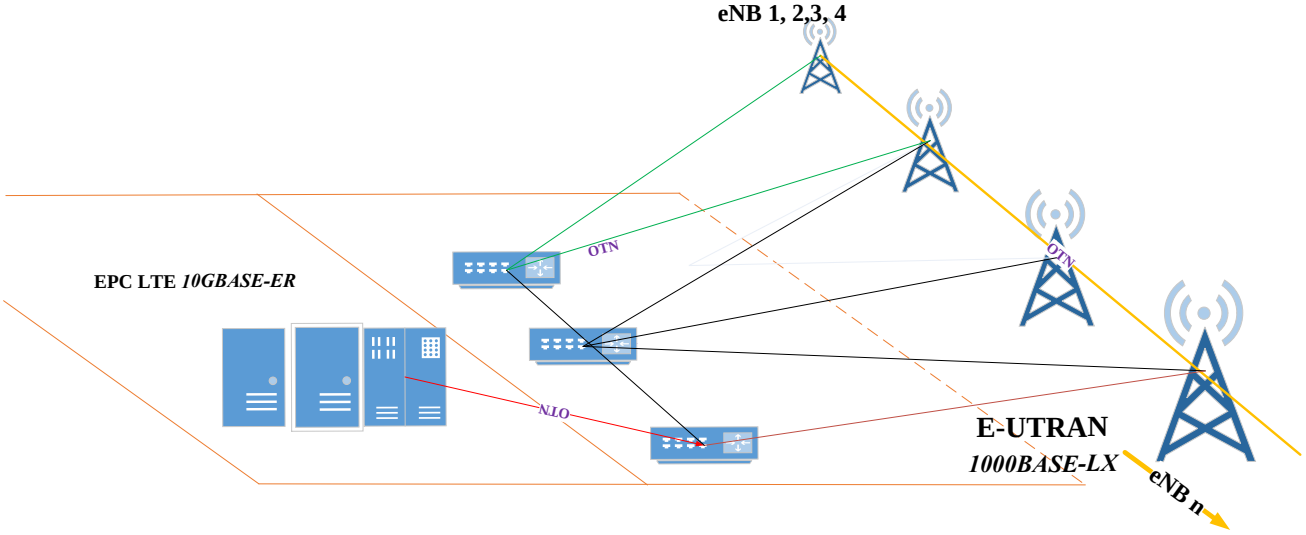


Рис.2 - Архітектура System Architecture Evolution

Але треба зазначити що IP мережа менш ефективна та має менш динамічну структуру керування що обмежує її в використання до мережі майбутнього FN.

Треба зазначити що будувати програмно – керовану мережу з нуля дуже дорого і накладна т.я. зупинити роботу вже працюючої інфраструктури неможливо.

Тому третя за популярністю вважається мережа OpenFlow де поверх вже існуючої інфраструктури можливо розташувати Мережу SDN і згодом розвивати вже Overlay мережу. Архітектура мережі OpenFlow

зображена на рис. 6.

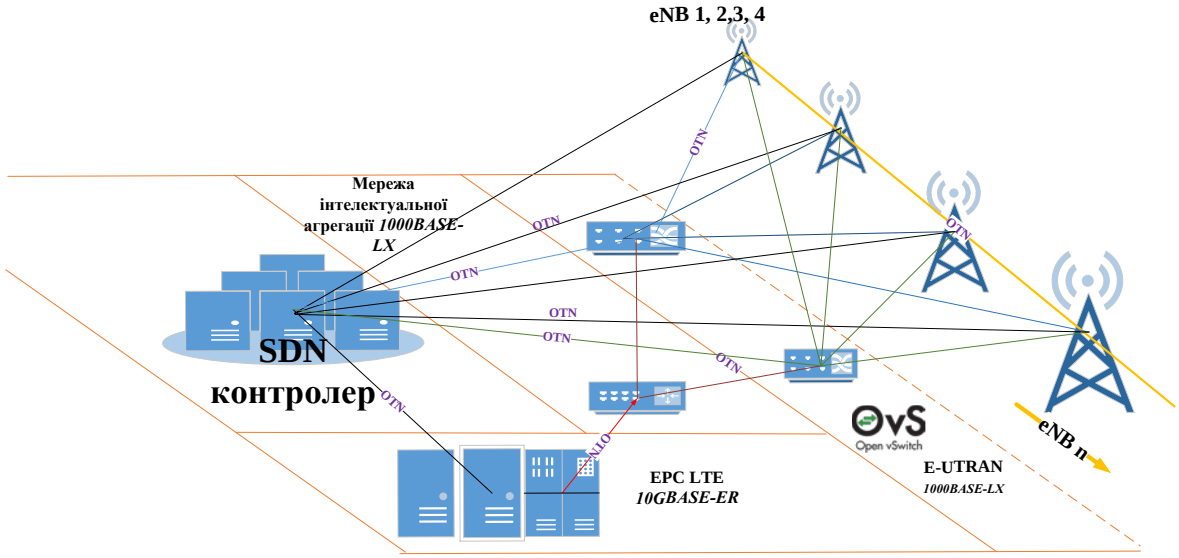


Рис. 3 - Гібридна архітектура SDN OpenFlow

Робота програмної частини частини SDN мережі

Програмно-конфігурується мережу (SDN від англ. Software-defined Networking, також програмно-обумовлена мережу) - мережа передачі даних, в якій рівень управління мережею відділений від пристроїв передачі

даних і реалізується програмно, одна з форм віртуалізації обчислювальних ресурсів.

Сучасні мережеві пристрої, складаються з трьох компонентів.

1. Рівень управління - це CLI, вбудований веб-сервер або API і протоколи управління. Завдання цього рівня забезпечити керованість пристроєм.

2. Рівень управління трафіком - це різні алгоритми і функціонал завданням якого є автоматична реакція на зміни трафіку т. Е. Інтелект пристрою.

3. Передача трафіку - функціонал забезпечує фізичну передачу даних.

Якщо централізувати управління трафіком, відокремивши управління від пристроїв і централізувати управління пристроями?

Гетерогенна комп'ютерна мережа - комп'ютерна мережа, що з'єднує персональні комп'ютери та інші пристрої з різними операційними системами або протоколами передавання даних. Наприклад, локальна мережа, яка з'єднує комп'ютери під управлінням операційних систем Microsoft Windows, Linux і MacOS, є гетерогенною[1][2]. Термін «гетерогенні мережі» також вживають у бездротових мережах, які використовують різні технології для підключення. Наприклад, бездротова мережа, яка забезпечує доступ через бездротову локальну мережу і здатна забезпечувати доступ, перемикаючись на стільниковий зв'язок, також називається гетерогенною мережею.

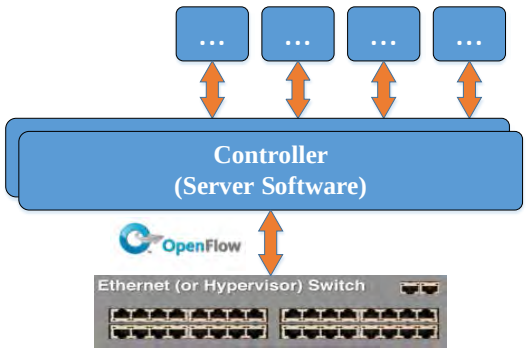


Рис.4 - Робота керування рівнями тренспортним сигментом SDNмережі

В результаті «новий» роутер або комутатор обслуговує тільки потік даних (рівень передачі трафіку DATAPLANE), ставати більш простим відповідно дешевшим. Звичайно ж позбавити повністю інтелекту мережеве пристрій не вийти, але його досить замінити простий таблицею переадресації (forwarding table).[7]

Програмно-орієнтована мережа має контролер SDN який відповідає за керування обладнанням за допомогою гіпервізора на якому встановлений це інтерфейс командного рядка CLI для окремих пристроїв для керування open virtual switch в архітектурі SDN, який який можливо реалізувати за допомогою API

Інтерфейс командного рядка (англ. Command line interface, CLI) - різновид текстового інтерфейсу (CUI) між людиною і комп'ютером, в якому інструкції комп'ютера даються в основному шляхом введення з клавіатури текстових рядків (команд), в UNIX-системах можливе застосування миші [1]. Також відомий під назвою консоль.

Інтерфейс командного рядка протиставляється системам управління програмою на основі меню, а також різним реалізаціям графічного інтерфейсу.

За допомогою прикладного рівня можливо покращити роботу мережі розробив додатки за допомогою яких контролер зможе розраховувати додаткові можливості. Та можливо впровадити ці додатки на прикладний рівень або на гіпервізор NFV.

Опис функціоналу, та додатки функцій

Програмно-керована мережа (SDN) – це універсальний термін, що охоплює кілька видів мережевих технологій, спрямованих на те, щоб зробити мережу гнучкою, як віртуалізована інфраструктура сервера і сховища сучасного дата-центру. Мета SDN – дати можливість мережевим інженерам і адміністраторам швидко реагувати на мінливі бізнес-вимоги. У мережі, яка визначається програмним забезпеченням, мережевий адміністратор може формувати трафік з централізованої консолі управління, не торкаючись окремих комутаторів, і може надавати послуги там, де вони необхідні в мережі, незалежно від того, які конкретні пристрої використовують сервер або інші апаратні компоненти пов'язані з ключовими технологіями впровадження.

Таблиця 1.

Таблиця програмованих і класичних мереж

Характеристика	Архітектура SDN	Класична архітектура IP
Програмованість	+	–
Централізоване	+	–

управління		
Конфігурація з помилкою	–	+
Комплексне управління мережею	–	+
Гнучкість мережі	+	–
Покращена продуктивність	+	–
Проста реалізація	+	–
Ефективна конфігурація	+	–
Вдосконалене управління	+	–

Надійність та контроль пристроїв у транспортному сегменті мобільної мережі

Незважаючи на високу надійність сучасних комп'ютеризованих системах, поява в них збоїв і відмов є цілком можливими подіями. Показники надійності програмно-керованої мережі, являє собою сукупність програмних і апаратних засобів які залежать один від одного і працездатність об'єкта залежить від їх функціонування та відмово стійкості. Комп'ютерна система це складний об'єкт який працює за послідовність виконання алгоритмів і команд які маніпулюють фізичним обладнанням , яке в свою чергу виконує функції транспорту потоків інформації.

Формат виведення інформації в інтерфейсі командного рядка виконується за допомогою CLI, та вбудований веб-сервер APIякий встановлений на гіпервізор.

А саме такі порушення роботи програмної частини контролера можуть виникнути під час роботи:

- неправильна модифікація або оновлення програмного забезпечення або додатка файлу системи,
- наявність IRSLKBDB програм в системі або в завантажувальних файлах,
- неузгодженість параметрів апаратної конфігурації з даними, записаними в пам'ять.
- неправильне розширення апаратної потужності SDN контролера ,
- відмова буферних IMC, що обслуговують потужнострумові IMC або периферійні пристрої.
- неузгодженість додатків програмного інтерфейсу API,

Внаслідок можливих збоїв і відмов після виконання завдання на контролера виникає питання про достовірність отриманої інформації. У зв'язку із цим всі сучасні системи мають засоби, що контролюють правильність функціонування як окремих пристроїв, так і ядра в цілому. Ці засоби одержали назву системи контролю SDN (в нашому випадку). Основними вимогами до системи контролю є: автоматичне виявлення факту неправильної роботи прикладної системи; усунення наслідків випадкових збоїв у процесі обчислень; локалізація місця відмови з точністю до змінного блоку.

Період роботи будь – якої складної системи можливо описати за допомогою кривої яку згідно теорії надійності прийнято називати типовою прямою. Ця пряма за допомогою цикл роботи об'єкта ділить на періоди де за кожний період система проходить визначений цикл, за допомогою якого можливо побачити стан надійності системи (рис. 5)

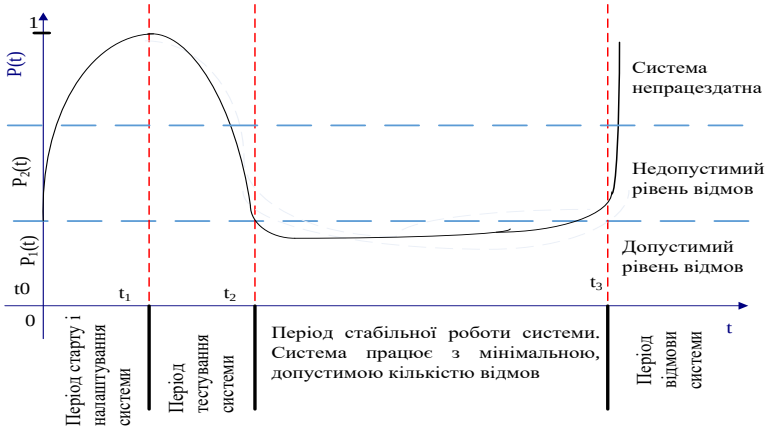


Рис.5 Типова пряма запуске SDN контролера.

Типова пряма показує .

1. Етапи запуску інфраструктури мобільної мережі, яка включає :

- період налаштування системи;
- період тестування системи;
- період стабільної роботи системи;
- період відмови системи.

2. Стан обєкта :
- стан непрацездатності системи ;
- недопустимий рівень відмов;
- допустимий рівень відмов;

1. Робочий стан мережі– мережа відповідає всім вимогам документації.

2. Неробочий стан мережою–мережа не відповідає хоча б одній вимозі документації на нього.(мережа може надавати послуги)

3. Працездатний стан мережі –мережа може виконувати всі задані для нього функції. (при цьому працездатний об'єкт може не задовольняти вимогам документації).

4. Непрацездатний стан мережі – коли значення хоча б одного параметра мережі, що характеризує виконуваність заданих об'єкту функцій, не відповідає вимогам документації.

Можливо частковий непрацездатний стан, при якому мережа здатна виконувати потрібні функції зі зниженими показниками (наприклад, вийшов з ладу один із свічів), або здатен виконувати лише частину потрібних функцій.

5. Граничний стан мережі – коли подальша експлуатація об'єкту недопустима чи не логічна або економічна невигодна подальше експлуатація обладнення.

Критерії граничного стану кожного об'єкта визначаються в документації на нього. Потрібно розуміти, що об'єкти можуть знаходитись в граничному стані і одночасно бути працездатним. В цьому випадку експлуатацію необхідно припинити.

P(A) – ймовірність виходу з ладу обладнення мережіSDN (непрацездатний стан)

A - подія

N – загальна кількість відмов

n – кількість відмов

Ймовірність достовірної події (обов'язково відбувається при кожному досліді)

$$P\{A_д\} = \frac{n_д}{N} = \frac{N}{N} = 1$$

Ймовірність неможливої події (не відбувається в жодному з дослідів)

$$P\{A_н\} = \frac{n_н}{N} = \frac{0}{N} = 0$$

1ймовірність випадкової події може змінюватись в межах $0 \le P\{A\} \le 1$ але ніколи $P\{A\} > 1$

Добутком подій називається складна подія, яка складається з того, що відбувається і подія, тобто відбуваються всі події. Така подія позначається:

$$A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_n = \prod_{i=1}^{n} A_i$$

Для незалежних подій справедлива рівність

$$P\left\{\prod_{i=1}^{n} A_i\right\} = \prod_{i=1}^{n} P\{A_i\}$$

Оскільки за означенням $P\{A\} \le 1$завжди, то ймовірність добутку менша найменшої ймовірності окремої події.

Сумою подій називається складна подія, яка має на увазі те, що відбудеться або подія, тобто виконається хоча б одна з подій. Сума подій позначається:

$$A_1 + A_2 + A_3 + \ldots + A_n = \sum_{i=1}^{n} A_i$$

Для незалежних подій справедлива рівність

$$P\left\{\sum_{i=1}^{n} A_i\right\} = 1 - P\left\{\prod_{i=1}^{n} \overline{A}_i\right\}$$

Розбиття на структурні блоки діючої мережі

Моделювання

Класична система не здатна адаптуватися за кількістю абонентів. Якщо вийде з ладу один з блоків.

Для більш точного разрахунку надійнісних характеристик програмно – керованої мережі, необхідно враховати як апаратну так і програмнуу час тину.

За період роботи (t) рис. 6 може збільшуватись кількість абонентів через це навантаження на свічі й контролери виростають за рахунок цього надійність системи падає . Також є фактор модернізації системи змінюються оптимальні та обхідні процеси маршрутизації, за рахунок чого можливі більші затримки та зростає ризик перевантаження вузлів та помилок програмної частини мережі.

Є періоди коли деякі помилки суттєві, або ділянки роботоючої схеми можуть нести не равномірну загрузки і мати більший коефіцієнт ізносу. Це треба враховати і аналізувати, або система буде виходити з ладу поступово і цей процес буде неконтролюючим. Та через деякий період ми не зможемо контролювати якість надання послуги.

Ппрограмний сегмент залежіть від апаратного саме послідовним зєдненням тому їх можливо розглядати окремо один від одного але потрібно врахувати що вони діють в програмно керованій мережі один на одного і не працюють при відмові якогось із рівнів як вказано на рис.6

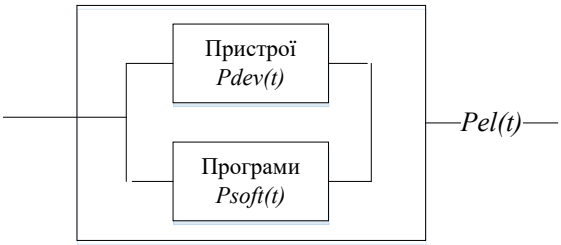


Рис.6 - Залежність програмного комплексу від апаратного

Залежність програмного і апаратного сегменту можливо охарактеризувати за формулою

$$P_{el}(t) = P_{dev}(t) \cdot P_{soft}(t) \qquad (1)$$

де: P_{el} –напрацювання до відмови однієї комірки мережі

P_{dev} - напрацювання до відмови апаратної частини мережі

P_{soft} - напрацювання до відмови програмної частини мережі

Цей процес можливо охарактеризувати як залежність програмного комплекту від апаратного. Апаратний комплекс в мережі SDN керує фізичним обладнанням тому працездатність по окремому сценарію неможлива. Роль централізованої системи робить програмний сегмент більш складним і значущим, в програмно-керованих мережах як що з ладу вийде контролер або контролери (як що вони резервуються або розносяться) система буде непрацездатною. Як що вийде з ладу контролер тимчасово можливо буде вирішити цей інцидент за допомогою обхідної маршрутизації але треба розуміти що несправність треба буде усунути як можна швидше т.я. критерії мережі будуть знижатися за рахунок відсутності оптимального вузла.

Для розрахунку надійності апаратної частини транспортного сегменту мобільної мережі ми маємо можливість використати Структурну надійність.

Структурна надійність будь-якого апарату - його результуюча надійність при відомій структурній схемі і відомих значеннях надійності всіх елементів, складових структурну схему.

На рисунку 7 зображена схема залежності апаратної частини системи від програмної, та гібридний метод який як правило і є домінуючим в складних системах типа мобільної мережі.

В систему контролю входять як програмні, так і апаратні засоби (рис.7). Програмний контроль базується на використанні програм, що дозволяють виявляти помилки, і ділиться на програмно-логічний і тестовий контроль.

Прикладами програмно-логічного контролю є метод подвійного обчислення, використання різного роду тотожних співвідношень. Тестовим контролем називають перевірку працездатності контролера за допомогою випробувальних програм, які бувають контролюючими і діагностичними.

Контролюючі тести призначені для виявлення факту несправності контролера, в той же час діагностичні тести служать для визначення місця несправності з точністю, наприклад, до змінного блоку.

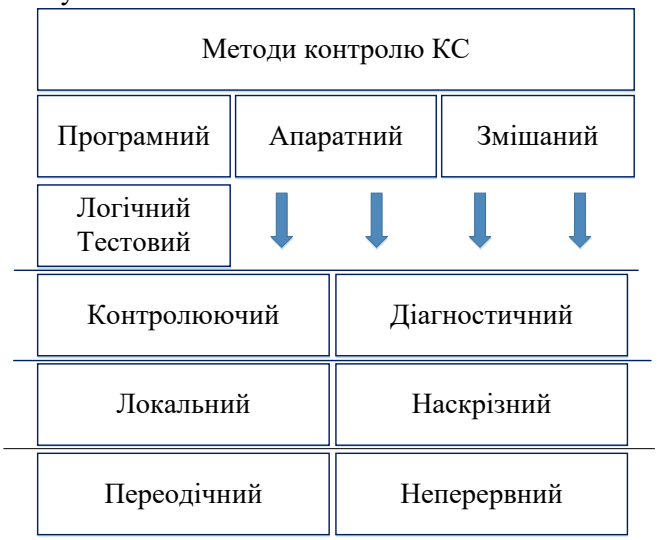


Рис.7 - Класифікація методів контролю КС.

Апаратним називають такий контроль, що здійснюється автоматично шляхом введення в контрольної апаратури. Як і програмний, він буває контролюючий і діагностичний.

Апаратні й програмні засоби контролю можуть бути наскрізними, коли контролюються всі без винятку вузли SDN, і локальними, коли контролюються окремі пристрої. Системи контролю можуть працювати безперервно або включатися періодично.

Апаратний і програмний методи контролю мають свої переваги і недоліки. Переваги програмних методів полягають у тому, що вони не вимагають включення до складу додаткового обладнання і, внаслідок цього, можуть бути застосовані в будь-якому типу мережі.. На відміну від програмних методів апаратний контроль не знижує продуктивності контролера, однак його використання вимагає додаткових апаратурних витрат. Тому в сучасних мережевих та компьютерних системах широко

використають комбінований програмно-апаратний контроль, що дозволяє при невеликих апаратурних витратах досягти високого охоплення контролем (до 95% всієї апаратури) [2]. При цьому виявлення і виправлення одиничних помилок, як правило, здійснюється апаратним контролем, а багаторазові помилки, виявлені як апаратним, так і програмним способами, усуваються .

Для контролю програмного забезпечення треба налаштувати автоматичний алгоритм роботи тестування програмного засобу, який зможе тестувати додатки API до того як ми їх використаємо в гіпервізорі.

В нашому випадку це можливо за допомогою віртуалізації NFV Network Functions Virtualization. Емалюються; робота мережі, потоків трафіку, процеси (які безпосередньо залежні від додатків).

Для оптимальної роботи мережі можливо використати **теорію визначення оптимального алгоритму маршрутизації** яка буде працювати на конкретному сценарії і на прикладному рівні розраховати який алгоритм є більш ефективним.

Резервування апаратної частини системи SDN

На рисунку 6 зображена схема роботи моделі, «Надійності системи мережі SDN»

Основний метод аналізу працездатності додатку – це його тестування. На рисунку 8 показано алгоритм тестування додатку за допомогою інформаційної технології

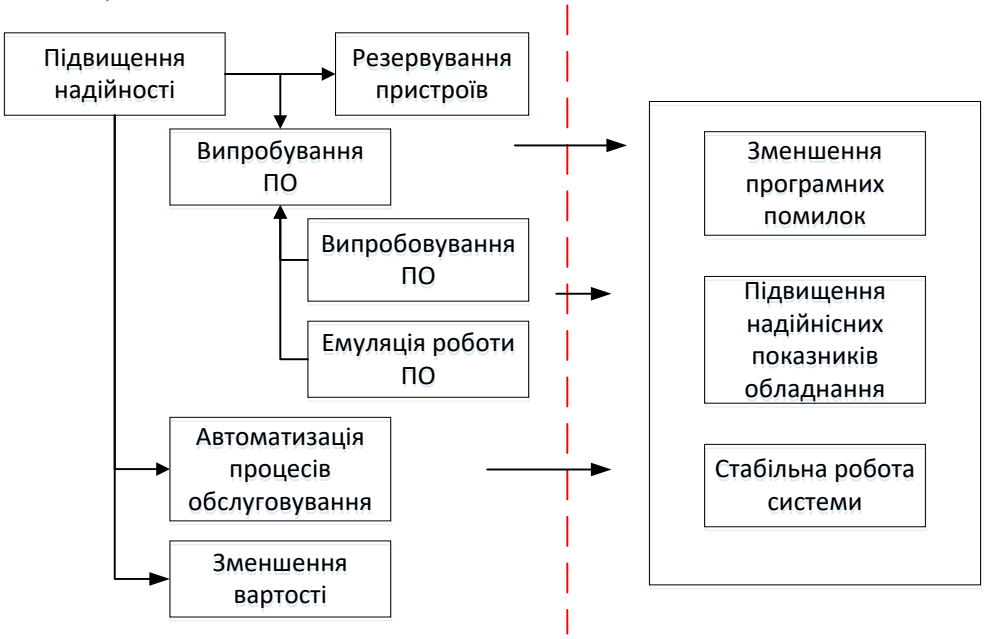


Рис.8 - Узагальнена структурно – логічна схема роботи моделі підвищення надійності SDN мережі

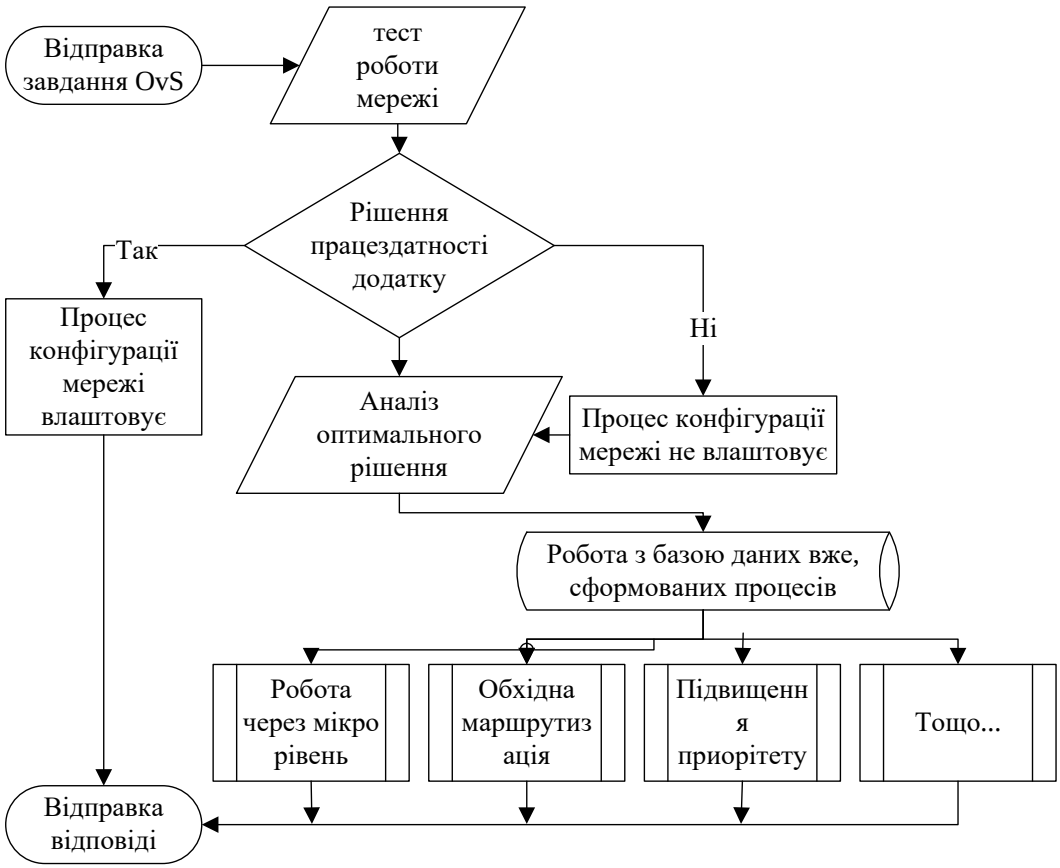


Рис. 9 - Приклад тестування додатку за допомогою інформаційної технології

При отриманні практичних даних система може контролювати стан мережі і тримати показники в межах встановленими користувачем або стандартом. Комплексне програмне забезпечення допоможе зменшити годину граничного стану мережі, зменшити терміни реконфігурації мережі, розрахувати затрати необхідні на ремонт або обслуговування обладнання.

Використовуючи першеобразні моделі (моделі про які йде річ а саме модель надійності та вартості компютерних мереж), можемо вивести додаткові функції, які будуть розраховати вартість ремонту та період подовження експлуатації після ремонту або технічного обслуговування.

Використовуючи першеобразні моделі: надійності та вартості комп'ютерних мереж (про них мова піде далі), можемо вивести додаткові функції, які будуть розраховати вартість ремонту та період подовження експлуатації після ремонту або технічного обслуговування.

Тестування додатків можливо виконати за допомогою алгоритму який також може аналізувати оптимальніший алгоритм для певного сценарію.

Реалізувати цей алгоритм можливо на прикладному рівні, на гіпервізорі NFV

Абстрактна схема будується по принципу розташування обєкту за його функціональними характеристиками.

Тобто як що об'єкт відмовить, стан всієї схеми не постраждає, це паралельні об'єкти зображено на рисунку 1а.

Якщо система вийде з лади при відмови блоку, це послідовна схема зображено на рисунку 1В.

Так як ми використовуємо централізовані системи, треба вказати що така система фактично являє собою послідовно розташованою блок схему зображено на рисунку 1D.

Та резервування системи рисунок 1 С

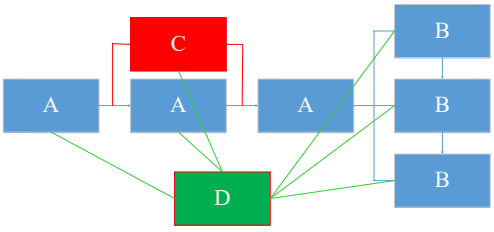


Рис.10 - Приклад розташування послідовної блок схеми

Основні недоліки підвищення надійності за допомогою методу резервування – це збільшення вартості та збільшення затримки за рахунок збільшення кількості вузлів, кожен з яких дає

затримку 0.022 мс., в програмно конфігурований мережах та (0,068 згідно імітаційному моделювання, та 0, 088.

На рис.11 бачимо результати моделювання мережі, до 99%, в даному случаї вартість мережі збільшується до 2х разів

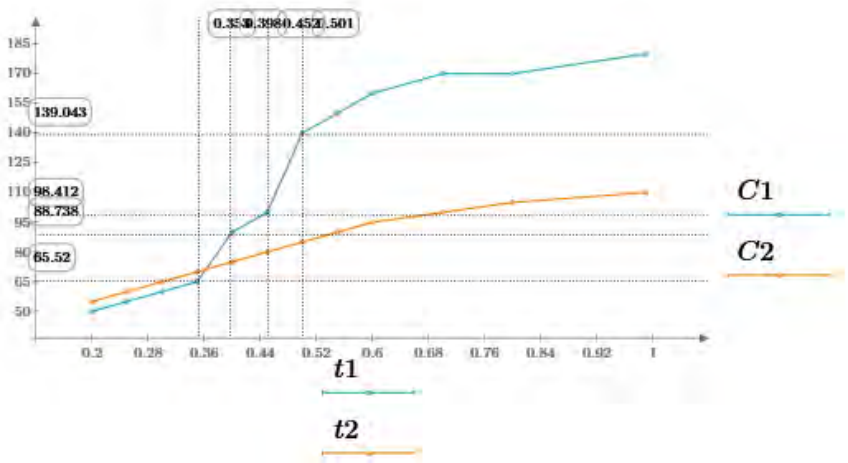


Рис.11 - Результат моделювання резервування системи, а саме підвищення надійності.

Для резервування контролеру необхідно долдати 30 % к вартості мережі. Для резервування кожного блоку, треба скористатися графіком та таблицею

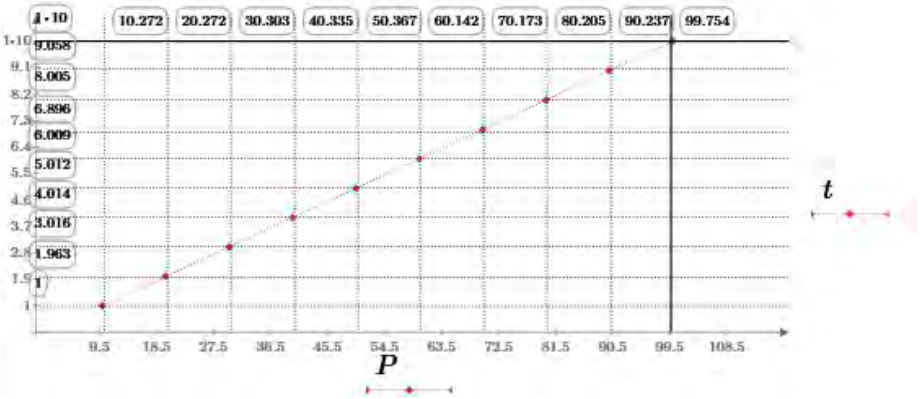


Рис.12 - Залежність надійності від вартості системи

Таблиця 2

Розразунок вартості резервувування системи SDN

	Вартість обл	Вартість обсл	Вартість ПО
Резервування контролеру	$(n+1)\cdot C_{con}$	$(E+1)\cdot C_{con}$	$+E$
Резервування OvS	$(n+1)\cdot C_{con}$	$(E+1)\cdot C_{con}$	$+E$
Інше	…	…	…
Загальне	$C_{dev}+E_{dev}+E=C_{cn}$		

де: n – кількість операцій, C_{dev} – вартість обладнання, E_{dev} - кількість операцій, E – вартість обслуговування

Залежність кожного додаткового блоку від затримки зображено на (рис.13). Кожний комутатор OvS додає затримку до 0.022-0.026мс. і зменьшує ефективність. Ефективність SDN при кількості комутаторів до 3х разів вища за IP тому для ефективного використання системи ми можемо продублювати кожний комутатор лише в 2 рази.

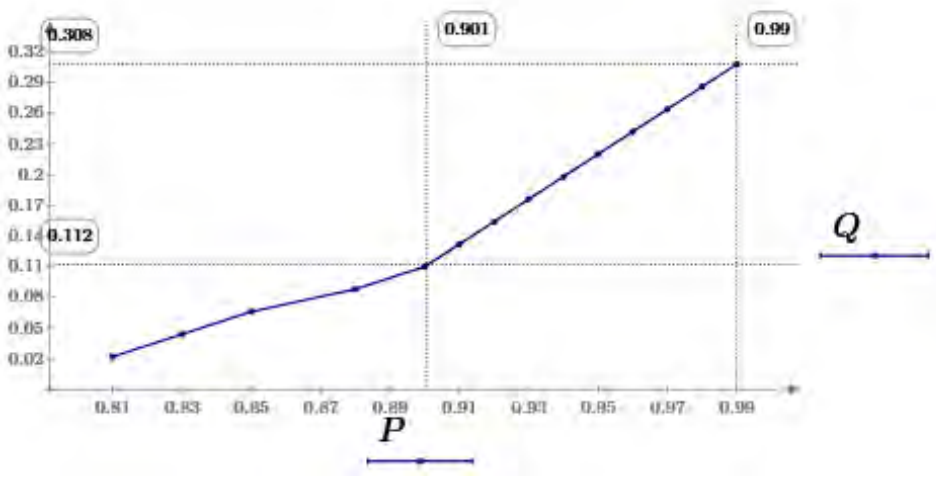


Рис.13 - Залежність кількісті комутаторів (затримка кожного комутатора) від затримки

5. ВИСНОВКИ

Надійність, показник динамічний, перемінна, характеристики об'єкту, зменшуються за тривалістю часу, саме за надійності.

Чим більше часу працює об'єкт, тим більше у нього негативних показників, таких як: відмова, часткова відмова, сбої в роботі як апаратної, так і програмної її частині, або рівня; і в крайньому випадку відмова.

Треба сказати що за часом обладнання старіє, як в апаратному так і в програмному, або як кажуть в «моральному» розумінні. Тобто це обладнання працювати не повинно, не тому що воно відмовило, а тому що за часом змінилось багато і стандартів і технологій.

Але на об'єкті, ми побачили, що процесом можливо керувати, за допомогою таких методів як резервування, та концентрацію навантаження. Зрозуміло що набагато ліпше робити керування програмним спосіб мережі SDN. Який ми саме розглянули, Та побудували архітектуру так названо гетерогенної мережі, яка накладаєтеся одна на одну, створюючи резервування децентралізованою мережею. Технологія ця має назву OpenFlow. Яка по ефективності На другому місті[5].

Виконані завдання розрахунку надійності мерами LTE за керуванням централізованих та децентралізованих методів керування цією мережею.

Та проаналізовано надійності характеристики мережі, яка керується за допомогою трьох способів, а точніше це IP мережі та SDN яка в свою чергу діляться на OpenFlow та Overlay .

Далі можливо розробити систему керування процесами обслуговування цієї системи, чим можливо керувати надійніними характеристиками об'єкту, та мати на увазі показники отказостійкості, критеріями чого являються, такі показники як, пропускна здатність, Таймінги сервісного затримання (0,08 сек, на маршрутизаторі наприклад.),годин напрацювання.

Треба зауважити що самою відмово стійкою являєтеся саме OpenFlow мережа, так як при виході із строю SDN контролера можна використати децентралізовану модель, то тіх пір доки мережа не буде відновлена.

6. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] В.Н. Азарсков, В.П. Стрельніков; "Надежность систем управления и автоматики," *Учебное пособие,* К.:НАУ,2004;

[2] Локозюк В.М. Савченко Ю.Г. Надійність; "Контроль, діагностика, і модернізація ПК," *Київ, видавничий центр «Академія»,* 2004.

[3] Погребинський С.Б., Стрельников В.П., "Проектирование и надежность многопроцесорных ЭВМ*," Радио и связь, Москва,* 1988;

[4] Вентцель Е.С., *Теория вероятностей,* Москва, Наука, 1969.

[5] Odarchenko, R., Abakumova, A., Polihenko, O., Gnatyuk, S., "*Traffic offload improved method for 4G/5G mobile network operator* , 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering," TCSET 2018 – Proceedings 2018-April, pp. 1051-1054

[6] Odarchenko, R., Abakumova, A., Tkalich, O., Ustinov, O. ,"LTE and wireless sensor networks integration in the concept of "smart home , 2016 IEEE 4th International Conference

Methods and Systems of Navigation and Motion Control," *MSNMC 2016* – Proceedings 7783100, pp. 35-38

[7] Василевський О.М., *Нормування показників надійності технічних засобів: навчальний посібник,* О.М. Василевський, В.О. Поджаренко.-Вініця : ВНТУ, 2010.- 129с.

Даков Сергій Юрійович асистент кафедри кібербезпеки та захисту інформації.

У 2011 році закінчив Бердянський державний педагогічний університет за спеціальністю «Комп'ютерні технологій та системи в управлінні та навчанні».

У 2013 Вступив до аспірантури, «Національного авіаційного університету», на кафедру «Інформаційної безпеки держави»

Наукові інтереси: інформаційна безпека, електроніка, розробка електронних схем, програмування контролерів, дистанційне та автоматизоване керування.

Дакова Лариса Валеріївна Доцент кафедри, кандидат технічних наук

Педагогічний стаж роботи в вищих навчальних закладах - 7 років.

Викладає дисципліни: "Цифрові системи телебачення та радіомовлення", "Мережі кабельного телебачення" та "Системи цифрового телерадіомовлення".

Здійснює керівництво атестаційними роботами студентів освітніх ступенів «бакалавр».