МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК
СЕКЦІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРОЕКТУВАННЯ

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «Інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів»

за спеціальністю 122 «Комп'ютерні науки»,
освітньо-професійна програма «Інформаційні технології проектування»

Виконавець роботи: студент групи ІТ.м-91 Щербань Тетяна Володимирівна

Кваліфікаційну роботу захищено на засіданні ЕК з оцінкою _____ «___» грудня 2020 р.

Науковий керівник _____ д.т.н., проф. Лавров Є.А.
(підпис)

Голова комісії _____ Шифрін Д.М.
(підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Суми-2020

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра комп'ютерних наук
Секція інформаційних технологій проектування
Спеціальність 122 «Комп'ютерні науки»
Освітньо-професійна програма «Інформаційні технології проектування»

ЗАТВЕРДЖУЮ
Зав. секцією ІТП

_____В. В. Шендрик
«___» _____ 2020 р.

ЗАВДАННЯ

на кваліфікаційну роботу магістра студентові

Щербань Тетяна Володимирівна
(прізвище, ім'я, по батькові)

1 Тема проекту *Інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів*

затверджена наказом по університету від «___»_____2020 р. № _____

2 Термін здачі студентом закінченого проекту «_07_» ___грудня___ 2020 р.

3 Вхідні дані до проекту літературні джерела з питань розроблення напівмарківських моделей, об'єктно орієнтованих моделей, експериментальні дослідження надійності інформаційних систем, статистичні дані негативного впливу на компоненти інформаційної системи.

4 Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) аналіз проблем забезпечення надійності, аналіз підходів та ймовірнісних характеристик, мета та постановка задачі, математичні моделі функціонування інформаційних систем в умовах внутрішніх вразливостей і конфліктних взаємодій, об'єктно-орієнтовані моделі конфліктної взаємодії, розробка імітаційних моделей конфлікту інформаційної системи і джерела негативного впливу.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) актуальність, апробація, характеристика проблеми та аналіз сучасних підходів та ймовірністних характеристик впливу, постановка задачі, розроблення математичних, об'єктно-орієнтованих моделей, розроблення імітаційних моделей, приклади, впровадження, висновки.

6. Консультанти випускної роботи із зазначенням розділів, що їх стосуються:

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

Дата видачі завдання _____.

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів випускної проекту	Термін виконання етапів проекту	Примітка
1	Ідентифікація ідеї проекту	01.09.20-18.09.20	
2	Аналіз предметної області	21.09.20-09.10.20	
3	Постановка задачі та планування робіт	09.10.20-26.10.20	
4	Розробка математичних моделей	02.11.20-20.11.20	
5	Розробка об'єктно-орієнтованих моделей	02.11.20-20.11.20	
6	Розробка імітаційних моделей	02.11.20-20.11.20	
7	Створення документації	12.10.20-01.12.20	
8	Здача пояснювальної записки	07.12.20	
9	Презентація проекту	21.12.20	

Магістрант _____ Щербань Т.В.

Керівник роботи _____ д.т.н., проф. Лавров Є.А

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: «Інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів».

Пояснювальна записка містить вступ, 4 розділи, висновки, додатки та список використаної літератури із 53 найменувань. Загальний обсяг роботи – 157 сторінок, у тому числі 85 сторінок основного тексту, 5 сторінок списку використаних джерел, 67 сторінок додатків.

Кваліфікаційну роботу магістра присвячено розробці інформаційної технології, що дозволяє визначати надійність інформаційної системи з урахуванням ряду гнучких налаштувань конфлікту. У роботі проведено аналіз предметної області, а саме характеристику проблеми надійності інформаційних систем при наявності вразливостей та аналіз імовірнісних характеристик конфлікту, чим і обґрунтовується актуальність роботи. У роботі виконана оптимізація математичних моделей, зокрема математична модель функціонування інформаційних систем з засобами захисту інформації, математична модель конфлікту інформаційної системи та коаліції джерел негативного впливу без та з інсайдером. Удосконалені та розроблені об'єктно-орієнтовані моделі конфліктних взаємодій, що перераховані вище. На основі даних моделей була виконана розробка імітаційних моделей можливих конфліктів. Результатом проведеної роботи є розроблені математичні, об'єктно-орієнтовані та імітаційні моделі функціонування інформаційних систем при наявному негативному впливу на них. Практичне значення роботи полягає у тому, що імітаційна модель ситуаційного конфлікту інформаційної системи і джерел негативного впливу дозволяє приймати обґрунтовані рішення з питань забезпечення надійності.

Ключові слова: імітаційна модель, вразливості, конфліктні взаємодії, негативний вплив, моделювання, інформаційна система.

ЗМІСТ

ВСТУП

Актуальність. Задачі аналізу та прогнозування надійності використання програмного забезпечення мають велике значення для організації стабільного функціонування інформаційних систем, використовуваних в всіх областях людської життєдіяльності. У той же час, існуючі алгоритми і моделі оцінки надійності програмного забезпечення інформаційних систем не в повній мірі враховують існуючу велику кількість факторів, які впливають на працездатність інформаційних систем в умовах конфліктних взаємодій.

Об'єкт. Надійність програмного забезпечення інформаційної системи в умовах навмисних негативних впливів.

Предмет дослідження. Ймовірнісні характеристики надійності використання програмного забезпечення.

Мета. Розробити інформаційну технологію аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів яка дозволяє врахувати динаміку зміни вразливостей, а також ряд інших параметрів, що визначають ситуаційний характер конфліктної взаємодії сторін.

Наукова новизна. На відміну від уже існуючих інтуїтивних підходів до аналізу вразливостей, розроблена модель побудована за принципом імітації процесу зміни станів системи, який залежить від організаційно-технічних характеристик системи забезпечення надійності.

Практична цінність. Імітаційна модель ситуаційного конфлікту інформаційної системи і джерел негативного впливу дозволяє приймати обґрунтовані рішення з питань забезпечення надійності.

Публікації. За матеріалами дослідження опубліковано 14 наукових робіт.

Апробації. Результати доповідались на 8 наукових конференціях:

– на студентській конференції «Перший крок у науку» (м.Суми, 24 лютого 2019 року);

– на науковій конференції «Інтелектуальний потенціал – 2019» (м.Хмельницький, 20-22 листопада 2019 року).

– на науковій конференції «Інформатика, математика, автоматика» ІМА 2019 (м.Суми, 23-26 квітня 2019 року);

– на науково-практичній конференції «Цифровые технологии в образовании, науке, обществе» (Петрозаводськ, 4-6 грудня 2018 року);

– на науковій конференції «Інтелектуальний потенціал – 2018» (м.Хмельницький, 14-16 листопада 2018 року);

– на науковій конференції «Інформатика, математика, автоматика» ІМА 2018 (м.Суми, 5-9 лютого 2018 року);

– на науково-практичній конференції «Цифровые технологии в образовании, науке, обществе» (Петрозаводськ, 27-30 листопада 2017 року);

– International Scientific Conference «UNITECH 2017» (17-18 November 2017, Gabrovo, Bulgaria);

Участь у конкурсах Всеукраїнських наукових робіт. Було взято участь у наступних Всеукраїнських наукових роботах:

– Всеукраїнського конкурсу студентських наукових робіт зі спеціальності 125 «Кібербезпека» 2020р.

– Всеукраїнський конкурс студентських наукових робіт зі спеціальності «Комп'ютерні науки» 2019/2020р.;

– Всеукраїнський конкурс студентських наукових робіт з Інформаційних технологій 27-28 березня 2019р.;

– Всеукраїнський конкурс студентських наукових робіт з галузей знань і спеціальностей у 2018/2019 навчальному році за спеціальністю «Кібербезпека» 5 квітня 2019р.;

– Всеукраїнський конкурс студентських наукових робіт з напрямку «Інформатика та кібернетика» 12-13 квітня 2018р.;

– Всеукраїнський конкурс студентських наукових робіт з галузей знань і спеціальностей у 2017/2018 навчальному році за спеціальністю «Кібербезпека» 27 квітня 2018р.;

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Характеристика проблеми забезпечення надійності інформаційних систем і технологій при наявності внутрішніх вразливостей

На сьогоднішній день питання збереження інформаційної безпеки є одним з найбільш актуальних не тільки в сфері інформаційних технологій і в галузях, де захист інформації завжди був одним з провідних ролей, а й у безлічі інших галузях. Корпоративні інфраструктури компаній, особливо великі, щодня піддаються змінам – з'являються нові вузли і цілі систем, змінюється топологія мереж і конфігурація обладнань. У цих динамічних системах є потреба в регулярному аналізі захищеності і негайному усуненні виявлених загроз безпеки.

Успіх джерел негативних впливів на інформаційні системи в цілому можна повністю визначити моментом часу, в якому використовується вразливість програмного забезпечення, а тому, визначення та детальне дослідження життєвого циклу вразливостей набуває особливої важливості [1-4]. Даний життєвий цикл необхідно описувати чи ж то датами подій чи самими цими подіями. У перерахованих далі роботах [1-4] списки цих подій відмінні не лише за кількістю, але і за складом подій, але, деякі важливі події відсутні у всіх таких таких списках чи ж то вони є включеними в інші події. У зв'язку з цим, був представлений перелік можливих подій на рисунку 1.1, що визначає життєвий цикл вразливостей. Він представляє собою об'єднані вже існуючі списки та додані відсутні події:

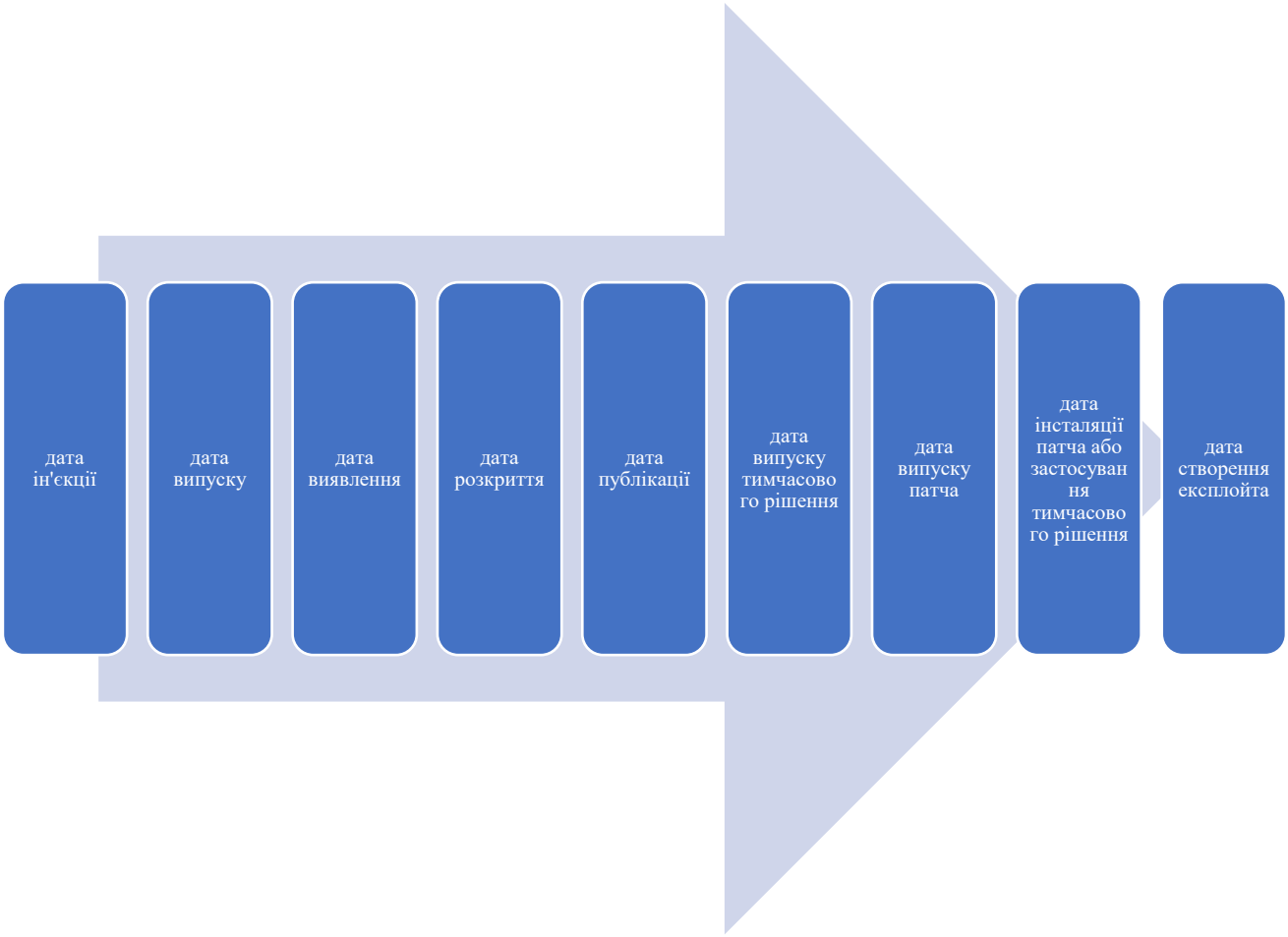


Рисунок 1.1 – Життєвий цикл вразливостей

Більшість з існуючих моделей, що оцінюють надійність програмного забезпечення, при розгляданні динаміки виявлення та усунення помилок у програмному забезпеченні, не виділяють помилки, за рахунок яких можливе здійснення навмисного негативного впливу. Вони не розглядають хоча б такий важливий параметр вразливості, як наявність інформації про її існування і характеристики. Якщо вразливість невідома, то нею не можна скористатися для негативного впливу, в той час як будь-яка інша помилка в програмному забезпеченні, навіть не будучи відомою, може призвести до порушень в його роботі. Відповідно до таких моделей при усуненні помилок з програмного забезпечення його надійність повинна зростати. Однак, на практиці в умовах конфліктних взаємодій з ростом часу експлуатації програмного забезпечення його надійність, як правило, падає, так як з ростом терміну експлуатації програми і відповідно її популярності збільшується

середня швидкість відкриття в ній нових вразливостей, в той час як середня швидкість їх усунення може залишатися незмінною і при закінченні підтримки програмного продукту розробниками зменшується до нуля.

Відповідно, залежно від того, чи настала вже та чи інша подія, вразливості можуть мати один або навіть кілька статусів одночасно. Нижче на рисунку 1.2 зображені на можливі статуси вразливостей.

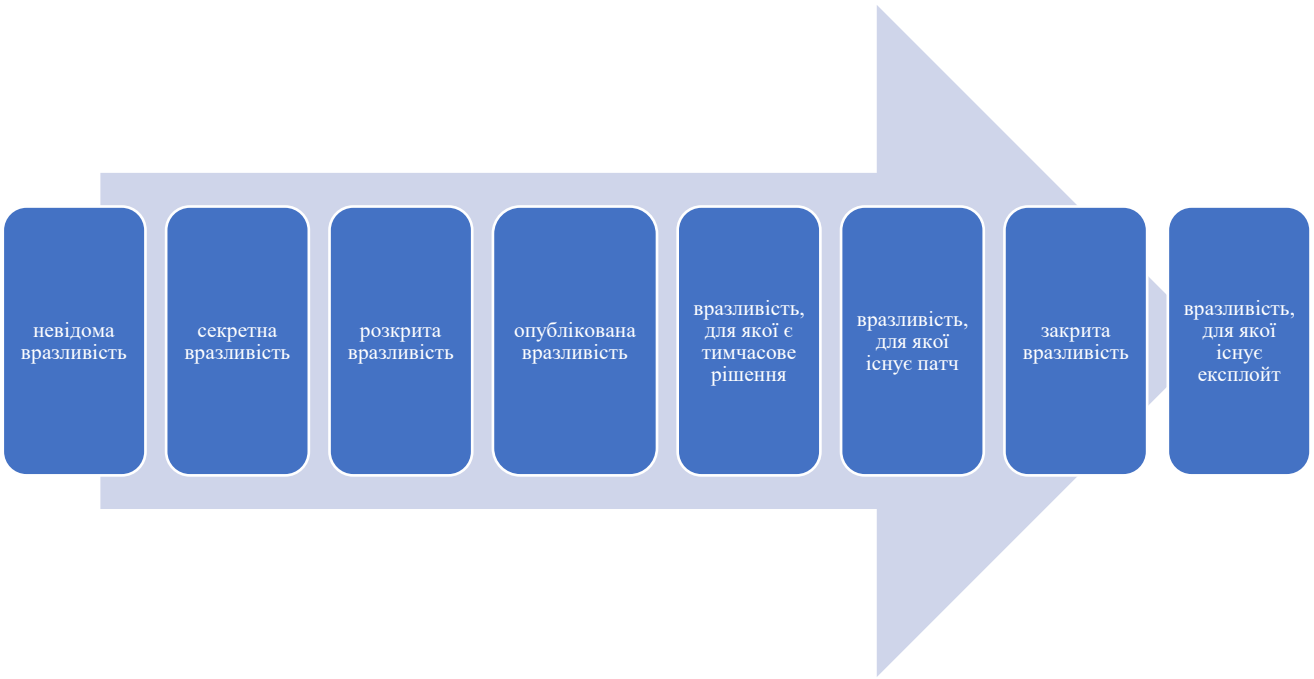


Рисунок 1.2 – Можливі статуси вразливостей

Як написано вище, у однієї вразливості може бути одразу відразу декілька статусів. Як приклад, у вразливості може в один в один і той же час бути патч та експлойт. Для ймовірної надійності однієї або іншої інформаційної системи визначальними в життєвому циклі вразливості є умови двух ключових моментів – виявлення дефектів та закриття дефектів. Уразливість не можливо використати джерелу, що здійснює негатвний вплив, якщо дефект ще не виявлений або вже закритий, а у випадку, коли ж він все таки виявлений, але ще не закрита, то відповідно – можливо.

Загалом, можна зазначити, що надійність інформаційної системи впливає як кількість відомих вразливостей в інформаційній системі, так і швидкість їх знаходження, а також простота використання джерелом негативного впливу, наявність захисту інформаційної системи, швидкість усунення вразливостей будь-яким чином.

1.2 Аналіз ймовірнісних характеристик негативного впливу в сучасних інформаційних системах

Для того, щоб провести характеристку умов функціонування сучасних інформаційних систем за наявних навмисних джерел негативного впливу, вважаю необхідним описати процес виявлення цих вразливостей, та як саме і для чого вони можуть використовуватися джерелами негативного впливу на інформаційну систему, та ймовірні шляхи усунення.

Виявлення вразливостей в інформаційній системі. У програмному забезпеченні зазвичай пошуком вразливостей займаються джерела негативного впливу, які використовують вразливості для різноманітних атак на інформаційні системи. До джерел можна віднести розробників програмного забезпечення, також спеціальні фірми, які працюють у галузі безпеки, а також інші зацікавлені в цьому люди або цілі організації. Але часто так трапляється, що вразливості можна знайти випадково, наприклад, звичайними користувачами під час користування будь-яким програмним забезпеченням [5].

Одним із важливих параметрів виявлення вразливостей є швидкість. Даний параметр має залежність як від заздалегідь відомих чинників, так і в цілому, наприклад, від якості написання коду, від рівня перевірки програмного забезпечення на наявність вразливостей під час тестувань ще до його офіційного запуску. На надійність впливає також кількість рядків у програмному коді, використання підходів

та технологій під час розробки. Але варто зазначити, що швидкість розкриття вразливостей залежить також від чинників, що змінюються в часі, а саме:

– поширення програмного забезпечення;
– якість випадкові фактори.

З останнього робимо висновок, що швидкість пошуку нових уразливостей залежить також від часу.

Оскільки в останній час все більше набирає популярності та лідирує операційна система Windows 10, що доводить статистика з [6-8] на рисунку 1.3, вважаю доцільним проводити подальші розрахунки використовуючи статистичні дані, що представлені у вільному доступі.

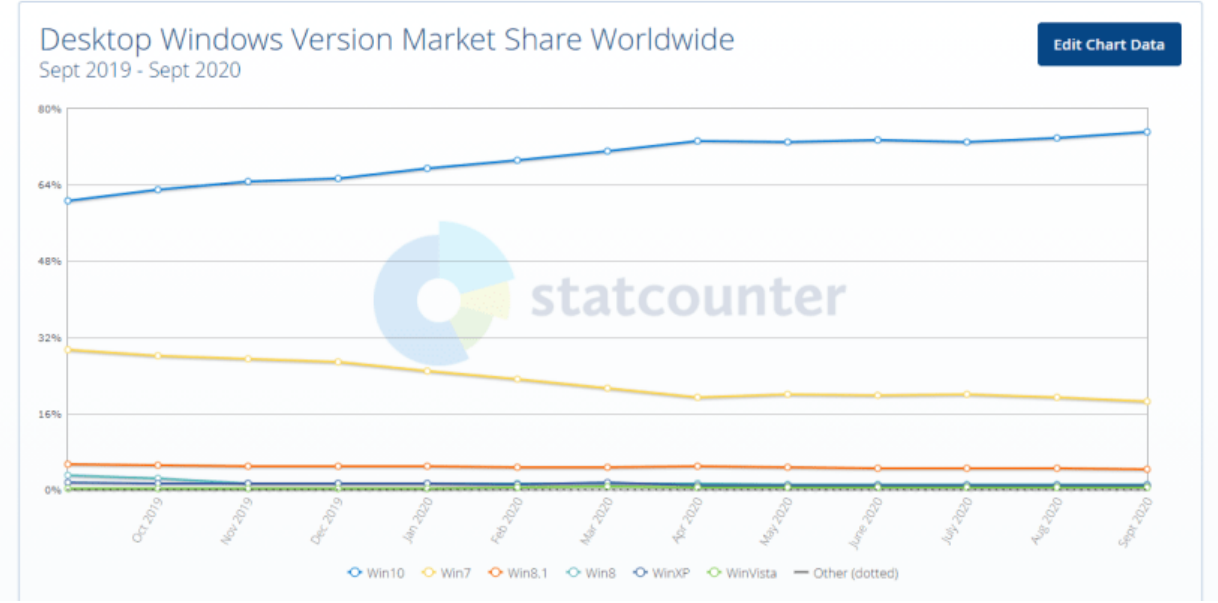


Рисунок 1.3 – Рейтинг операційних систем

Нижче на рисунках 1.4-1.5 приведені дані щодо щорічних виявлень вразливостей в операційній системі Windows 10.

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2015	57	4	19	6	6					10	5	26			
2016	172	6	47	23	7					19	31	82			
2017	268	32	50	16	2		1			18	108	19			
2018	257	21	45	19	1		1			39	72	1			
2019	357	28	124	101	6		1			10	73	2			
Total	1111	91	285	165	22		3			96	289	130			
% Of All		8.2	25.7	14.9	2.0	0.0	0.3	0.0	0.0	8.6	26.0	11.7	0.0	0.0	

Рисунок 1.4 – Статистичні дані знайдених вразливостей у Windows 10

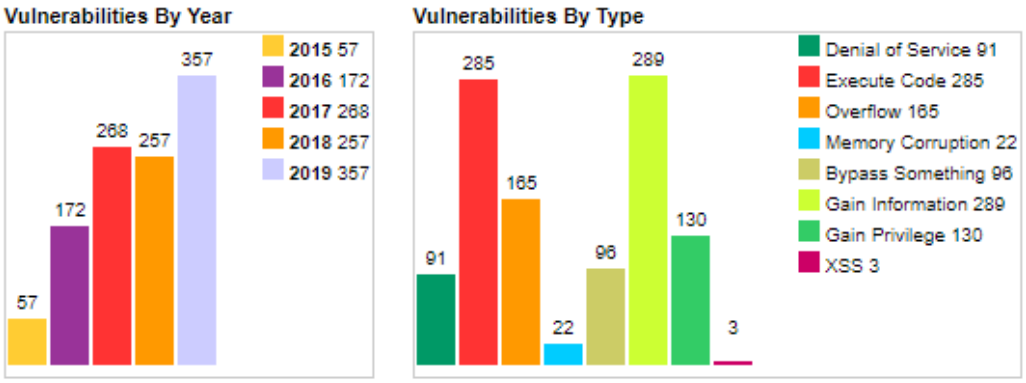


Рисунок 1.5 – Діаграми вразливостей у Windows 10 по типу і по роках

На основі цих даних не важко порахувати середньорічну швидкість виявлення вразливостей у Windows 10. Занесемо дані у таблицю 1.1.

Таблиця 1.1 – Середньорічна швидкість виявлення вразливостей у Windows 10

Період життя програмного забезпечення, рік	Середньорічна швидкість виявлення вразливостей, од/місяць
1	4.75
2	14.3
3	22.3
4	21.4
5	29.75

Поширення інформації про вразливості і її можливе використання. Те, що вирішить зробити з інформацією особа, яка знайшла вразливість, залежить від її

внутрішніх принципів, а також зовнішніх обставин. Варіантів поведінки може бути безмежна кількість, але в зведеному вигляді їх можна виокремити п’ять [9,10]:

– виставити інформацію про вразливість на продаж на "чорному" ринку вразливостей;

– розкрити інформацію про вразливість джерелу негативного впливу безкоштовно або ж самому її використати в кримінальних цілях;

– самостійно опублікувати вразливість;

– безкоштовно сповістити інформацію про вразливість вендору;

– виставити вразливість на продаж на "білому" ринку вразливостей.

Шляхи потенційного поширення інформації про вразливості та варіанти їх ймовірного використання показані на рисунку 1.6.

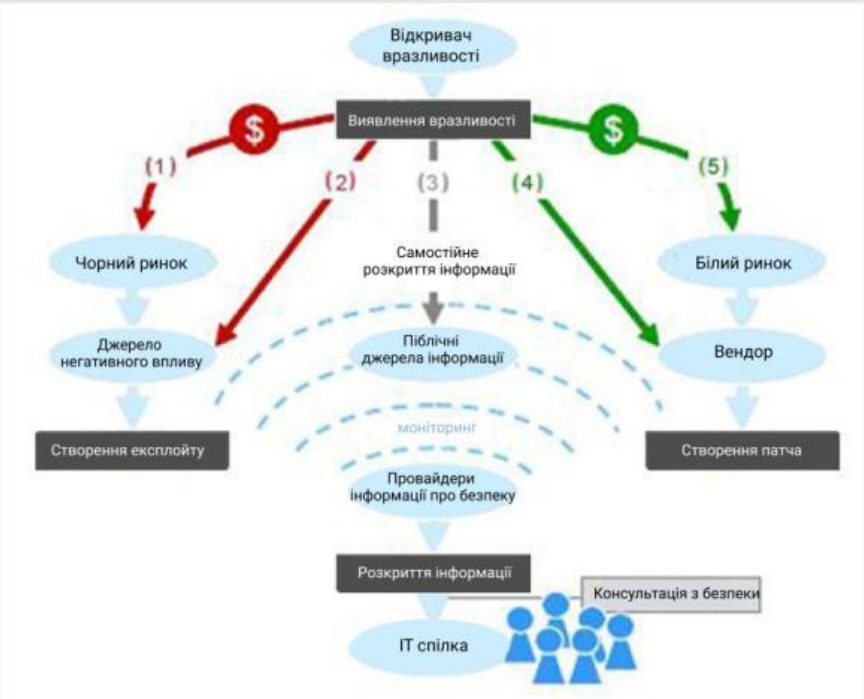


Рисунок 1.6 – Поширення інформації про вразливість

Провайдери інформації про безпеку. У зв’язку зі стрімким розвитком кіберкримінала, фірми і приватні користувачі постійно потребують точної і перевіреної інформації про вразливість для оцінки ризику та захисту свого власного програмного забезпечення. Інформацію про вразливість можна дізнатися на сайтах

вендорів, на порталах безпеки, зі спеціальних електронних розсилань, на конференціях по надійності і безпеці, з блогів експертів і безлічі інших джерел. Однак, для більшості фірм і користувачів моніторинг всіх цих джерел для отримання важливої для них інформації про безпеку незручний з економічної та інших точок зору. Тому з перших років існування мережі Інтернет деякі приватні та урядові організації спеціалізуються на зборі та публікації інформації про вразливості. Деякі з цих організацій відкривають науково-дослідні лабораторії безпеки, торгують засобами забезпечення надійності, наприклад, системами виявлення проникнення, антивірусним програмним забезпеченням, або надають платні послуги щодо забезпечення надійності та консалтингові послуги. Ці організації проводять ефективний моніторинг різних джерел інформації про вразливість, перевіряють знайдений контент і публікують їх відкриття як консультації з безпеки, які описують вразливості в стандартизованому форматі. Ці організації відіграють дуже серйозну роль в забезпеченні надійності роботи інформаційної системи[11].

Організація негативних навмисних впливів за допомогою вразливостей. У загальному випадку реалізація навмисного негативного впливу на інформаційну технологію або систему включає декілька етапів [12]. Джерелом негативного впливу будемо називати зловмисника або звичайного тестувальника системи, чи користувача, що допускає помилки під час роботи системи.

Можна виділити п’ять основних фаз реалізації негавтиного впливу зловмисником, що зображені на рисунку 1.7.

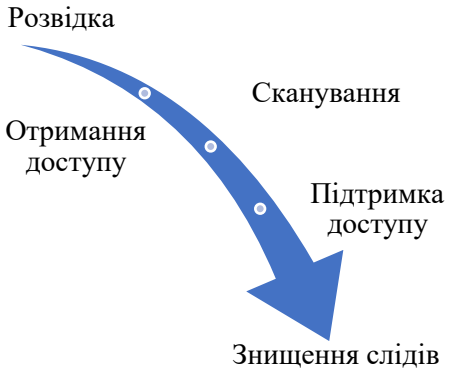


Рисунок 1.7 – Основні фази реалізації негативного впливу

Під час «розвідки», тобто першої фази, джерело негативного впливу шукає та накоплює інформацію про інформаційну систему, користуючись при цьому активними або пасивними засобами. Далі, під час наступної фази, що називається «скануванням» джерело негативного впливу приступає до активного штурмування інформаційної системи задля пошуку вразливостей, можливих для використання. Далі відбувається фаза «отримати доступ», коли виявлена вразливість, джерело негативного впливу використовує її, для того щоб заполучити доступ до інформаційної системми. Потім – відбуваєтьсч фаза «підтримки доступу». Щойно з'являється доступ до інформаційної системи, джерело негативного впливу одразу намагається підтримувати доступ для того до самої реалізації мети негативного впливу. А вже після – відбувається «знешкодження слідів», коли джерело, що здійснило негативний вплив, всіляко знищує усі можливі докази про здійснену атаку.

Не всі з представлених 5 етапів обов'язкові, так як в 4-му і 5-му випадках система вже пошкоджена, а тому, з позиції аналізу надійності інформаційної системи, що оцінюється, видається доречним розділити навмисний негативний вплив на 3 етапи [12,13]:

– визначення в програмному забезпеченні, що встановлене в інформаційну систему;

– визначення хоча б однієї вразливостей в програмному забезпеченні;

– визначення способу, як використати вразливості для здійснення негативного впливу на інформаційну систему.

Таке представлення навмисного негативного впливу дозволить охарактеризовувати джерело негативного впливу за допомогою середнього часу, що необхідний йому на кожен з перерахованих етапів. До того ж на дані проміжки часу буде впливати кваліфікація джерела негативного впливу з одного боку, та рівень його обізнаності про інформаційну систему з іншого боку,.

Практично, здійснювати навмисно негативний вплив на систему може не одне джерело негативного впливу, а цілі команди, які можуть розподіляти етапи праці між

собою, що має також бути враховуваним під час аналізу надійності інформаційної системи.

Під час здійснення негативного впливу з боку джерела відповідного впливу, дефект, який джерело спробує використати, може бути закритий за допомогою адміністратора інформаційної системи, через що джерело негативного впливу не зможе закінчити успішну атаку. Це означає, що від швидкості, з якою будуть закриватися вразливості в програмному забезпеченні, що встановлено в інформаційній системі, надійність буде прямопропорційно залежати цієї системи.

До того ж можливо, що інформаційна система матиме певний рівень захисту, тобто в ній будуть встановлені спеціальних засоби інформаційного захисту. По відношенню до цього, джерела негативних впливів поділяються на зовнішні та внутрішні. Зовнішні джерела негативного впливу представляють собою такі джерела, яким першим чином необхідно здійснити негативний вплив на засоби, що захищають інформацію, а вже після цього і на саму інформаційну систему для завдання успішного негавтиного впливу, тим самим подолавши захист, використовуючи вразливості в її програмному забезпеченні та засобах захисту інформації. Внутрішніми джерелами негативного впливу будемо називати ті джерела, які можуть здійснювати негавтиний вплив на інформаційну систему відразу, напряму, використовуючи дефекти програмного забезпечення. Також існують випадки, коли у системі встановлені та використовуються хитрі системи обману джерел, тобто підставляється підроблена система замість реальної, а тому спочатку джерела негативного впливу не розуміють і проводять штурм та пошуки вразливостей в підробленій системі, до тих пір, поа не зрозуміють, що ця система несправжня. Усі ці можливі варіанті слід враховувати під час розробки моделей та алгоритмів для аналізу надійності застосування програмного забезпечення в інформаційних системах за умовах конфліктної взаємодії із негативним впливом [14].

Усунення вразливостей з інформаційної системи. Для того, щоб усунути вразливість з інформаційної системи, адміністратору інформаційної системи треба деінсталювати програмне забезпечення, яке містить вразливість, або застосувати

патч, який створюється компанією, що впускає програмне забезпечення, щоб усунути цю вразливість або застосувати швидке будь-яке рішення, що запобігає можливості використання вразливості. Зазвичай, такі рішення оприлюднюють розробники програмного забезпечення.

Пошук та установку патчів проводять системні адміністратори самостійно або через спеціальні програми, які оновлюють програмне забезпечення.

Системні адміністратори можуть користуватися сканерами дефектів та для захисту встановлювати спеціальне програмне забезпечення. У цьому випадку джерелу негативного впливу спочатку необхідно зламати це спеціальне програмне забезпечення, використовуючи вразливості, які в ньому є перед зломом самої системи.

Організації можуть замовляти послуги у "етичних" або "білих" джерел негативного впливу, щоб знайти слабкі місця в інформаційній системі, більше навіть для того, щоб виявити дефекти, які ще невідомі нікому та власне їх усунути [12,13].

Проміжок часу, за який буде усунуто дефекти, залежить від декількох моментів. З однієї стороні, це рівень технічної підтримки програмного забезпечення, що включає швидкість, з якою створюються патчі та випускаються тимчасові рішення вендорами, а з іншої сторони – це рівень адміністратора програмного забезпечення, його виконання обов'язків чи кваліфікація, ті чинники, які визначають швидкість встановлення патчів та вчасне використання тимчасових рішенн, які зможуть забезпечити усунення дефекту, а також можливість адміністратора самостійно чи з використанням спеціальних інструментів виявляти та знешкоджувати вразливості у встановленому програмному забезпечнні.

Нижче на рисунку 1.8 продемонстровано узагальнену структурну схему основних процесів та суб’єктів, які можуть здійснювати значний вплив на надійність інформаційної системи та використаних в них програмних забезпечень.

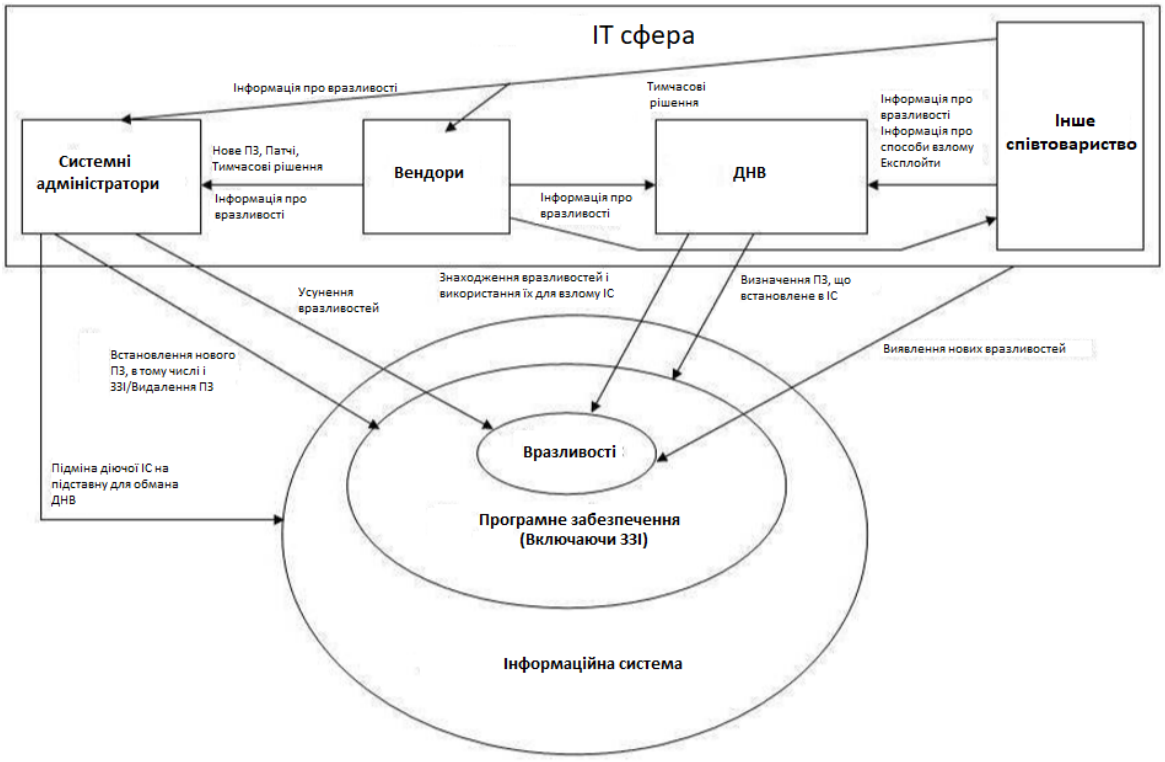


Рисунок 1.8 – Схема впливових процесів на надійність інформаційної системи

З вищезазначеного слідує, що дуже велика кількість факторів впливають на надійність роботи інформаційної системи.

Більша частина цих чинників має характер, який визначаться випадковим чином, а тому дана умова повинна обов’язково бути врахована у моделях.

Очевидно, що інформаційна система не може функціонувати статично, вона є змінною у часовому ресурсі. Змінюється швидкість знаходження та усунення дефектів, рівень досвіду джерел негативного впливу, тому моделі, які статично описують стан інформаційних систем є недостовірними.

Так як більша частина характеристик, за допомогою яких описується робота інформаційної системи, залежать від часового ресурсу, то надійне функционування інформаційної системи з наявним навмисним негативним впливом буде визначатися не за допомогою поточних значень даних параметрів, а з використанням майбутніх. Мається на увазі період часу, для якого буде проводитится аналіз надійності роботи інофрмаційної системи.

Моделі, за допомогою яких описується поведінка інформаційної системи при конфлікті з навмисним негативним впливом, повинні враховувати динаміку конфліктної взаємодії між різними суб'єктами, які беруть участь в цих процесах[15,16], а не лише динаміку окремих процесів. З цього слідує, що процес закриття вразливостей безпосередньо впливає на процес використання вразливостей для навмисного негативного впливу.

Головною вимогою до алгоритмів та моделей, що необхідно створити є: легке удосконалення алгоритмів і моделей, модифікація яких не потребує серйозних змін в їх концептуальній складовій, так як існує безліч ситуацій і необхідно передбачити можливість застосування додаткових обмежень та можливих умов реалізації конфліктної взаємодії. Створені алгоритми та моделі повинні враховувати параметри з доступних джерел даних, що можна знайти у відкритому доступі.

1.3 Аналіз сучасних підходів до оцінки надійності інформаційних систем і технологій в умовах негативних впливів

На даний час є величезна кількість підходів щодо аналізу надійності за умов негативних впливів і до окремих інформаційних технологій [17-18], і в цілому до інформаційної системи. У цій роботі значна увага приділяється аналізу підходів [17-20], які так чи інакше стосуються питання можливого використання джерелом вразливостей програмного забезпечення для здійснення зовнішніх негатвиних впливів, що можуть порушувати працездатність інформаційної системи, тому що у більшості вже відомих робіт увага приділена аналізу впливу будь-яких дефектів програмного забезпечення на надійність системи [17-19].

Можна визначити три категорії даних підходів:

– підходи, що відповідають нормативам, офіційно підкріплені документами та мають державний або міжнародний рівень;

– підходи, що актуальні на ринку послуг комп'ютерної безпеки;

– підходи, що на даному етапі несуть тільки науковий сенс.

Порівнюючи різні підходи, необхідно зауважити той момент, наскільки повно ними враховуються справжні обставини функціонування інформаційної системи, коли присутній навмисний негативний вплив, яка кількість чинників ними враховується, що це за фактори і власне як вони впливають.

З огляду на вищезазначене, нижче представлений перелік критерій за якими можна порівняти підходи щодо аналізу надійності інформаційних систем при навмисному негативному впливі:

– враховані динамічні показники надійності інформаційної системи (іншими словами, що саме враховується – процеси чи точні стани інформаційної системи);

– процеси, що враховуються;

– врахування недетермінованого характеру процесів;

– врахування параметрів, від яких можуть залежати процеси;

– оцінювання параметрів, які враховуються (оцінювання відбувається на основі прогнозу або ж наявної статистики).

Якщо порівняти підходи щодо аналізу надійності інформаційної системи при цілеспрямленій атаках негативного впливу програмного забезпечення, то можна виділити дві категорії:

– статичні підходи;

– динамічні підходи.

Особливістю статичних підходів є врахування ними лише конкретного, тобто, зазвичай, поточного стану інформаційної системи. Це означає, що оцінка надійності інформаційної системи відбувається на основі аналізу поточних умов функціонування інформаційної системи. При цьому має бути передбачено, що змін в поточних умовах функціонування інформаційної системи не має бути, але все таки у випадку таких змін, вони мають бути затвердженими адміністратором інформаційної системи, що дозводить їм швидко та ефективно в цих нових обставинах проаналізувати надійність інформаційної системи. Але основною проблемою при

даному підході є те, що дуже велика кількість змін в умовах функціонування інформаційної системи не залежить від адміністратора. Можна виділити три процеси, від яких залежить надійність інформаційної сиситеми:

– виявлення в програмному забезпеченні вразливостей;

– використання виявлених вразливостей джерелом негативного впливу для навмисного негативного впливу на інформаційну систему;

– закриття виявлених вразливостей

– динаміка конфлікту між процесом закриття і процесом навмисного негативного впливу на інформаційну систему.

Так як адміністратори інформаційної системи можуть здійснювати вплив лише на процес безпосереднього закриття вразливостей шляхом встановлення патча або винайдення тимчасового рішення, зазвичай, вони стають залежними від вендора, що займається цим програмним забезпеченням, де була виявлена вразливість. Тому що лише компанія. Що займається розробкою продукту, може випустити повноцінний сертифікований патч або тимчасове рішення проблеми. Єдиним моментом може бути випадок, коли адміністратор має досить високу кваліфікацію та досвід, щоб власноруч спробувати розробити або знайти рішення для хоча б тимчасового усунення вразливості до моменту випуску патча.

Тому, фактично, можна виділити ряд недоліків при використанні статичних підходів:

– не враховування в інформаційній системі динаміки процесу виявлення і закриття вразливостей;

– не враховування динаміки навмисного негативного впливу на інформаційну систему;

– не враховування динаміки конфліктної взаємодії між джерелом негативного впливу, яке намагається нанести навмисний негативний вплив на інформаційну систему та системним адміністратором, який працює над закриттям вразливостей.

На відміну від статичних підходів, динамічні [19,21-22] розглядають не показники, які представляють конкретні стани інформаційної системи, а ті, що характеризують саме процеси, які можуть вплинути на надійний стан інформаційної системи.

Прикладом цього є модель, яка заснована на теорії масового обслуговування [19] та описує динаміку появи вразливостей в інформаційній системі, а також модель конфлікту джерела негативного впливу і інформаційної системи [21] або модель оцінювання надійності сиситеми, яка захищає інформацію від несанкціонованого доступу [22].

Модель, за допомогою якої описується динаміка появи вразливостей в інформаційній системі, сформована на основі теорії масового обслуговування. У [23] запропонано представити процес виявлення нових дефектів та подальшого усунення як робота системи масового обсдуговування. З інтенсивністю λ, вхідним параметром задається пуассоновский потік вразливостей, і за допомогою засобів масового обслуговування з інтенсивністю μ дані вразливості обслуговуються. Варто зазначити, що відразу ж після виявлення кожної вразливсоті починається пошук шляхів її усунення, а тому число каналів представленого засобу масового обслуговування є нескінченнім числом. З урахуванням цих припущень можна визначити ймовірність відсутності вразливості, що знаходиться у системі становить [23]:

$$P(0) = \frac{1}{1 + \sum_{n=1}^{\infty} \frac{1}{n!} \left(\frac{\lambda}{\mu} \right)^n}, \quad (2.1)$$

А з урахуванням формули:

$$e^x = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}, \quad (2.2)$$

вираз (2.1) набуває вигляду:

$$P(0) = e^{-\frac{\lambda}{\mu}}. \quad (2.3)$$

Для того, щоб оцінити параметри моделі [23], а саме з якими інтенсивностями λ відкриваються вразливості та з якими інтенсивностями μ вони закриваються, пропонується використовувати поточні статистичні дані [23].

Таким чином, запропонований у [23] підхід не враховує декілька важливих факторів, які можуть мати великий вплив:

– не враховується зміна параметрів процесів виявлення та усунення вразливостей з часом. Для того, щоб можно було проводити аналіз надійності інформаційної системи точніше, є необхідним здійснення прогнозу на період оцінки для цих параметрів;

– не враховується залежність надійності інформаційної системи від властивостей джерела негативного впливу, які можуть виконувати негативні на цю інформаційну систему впливи. У тому числі не враховується ні кількість джерел негативного впливу ні розподіл праці між ними.

Модель конфлікту джерела негативного впливу та інформаційної системи, розглянута в [21], представляє собою випадковий напівмарківський процес, що зображено нижче, на рисунку 1.9, основу якого складає концептуальна модель конфлікту інформаційна система – джерело негативного впливу, що продемонстровано на рисунку 1.10.

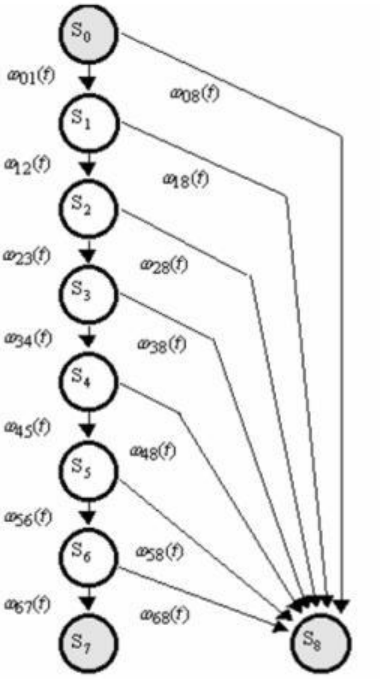


Рисунок 1.9 – Опис конфлікту конфлікт джерела негативного впливу і інформаційної системи за допомогою напівмарсківського процесу [21]

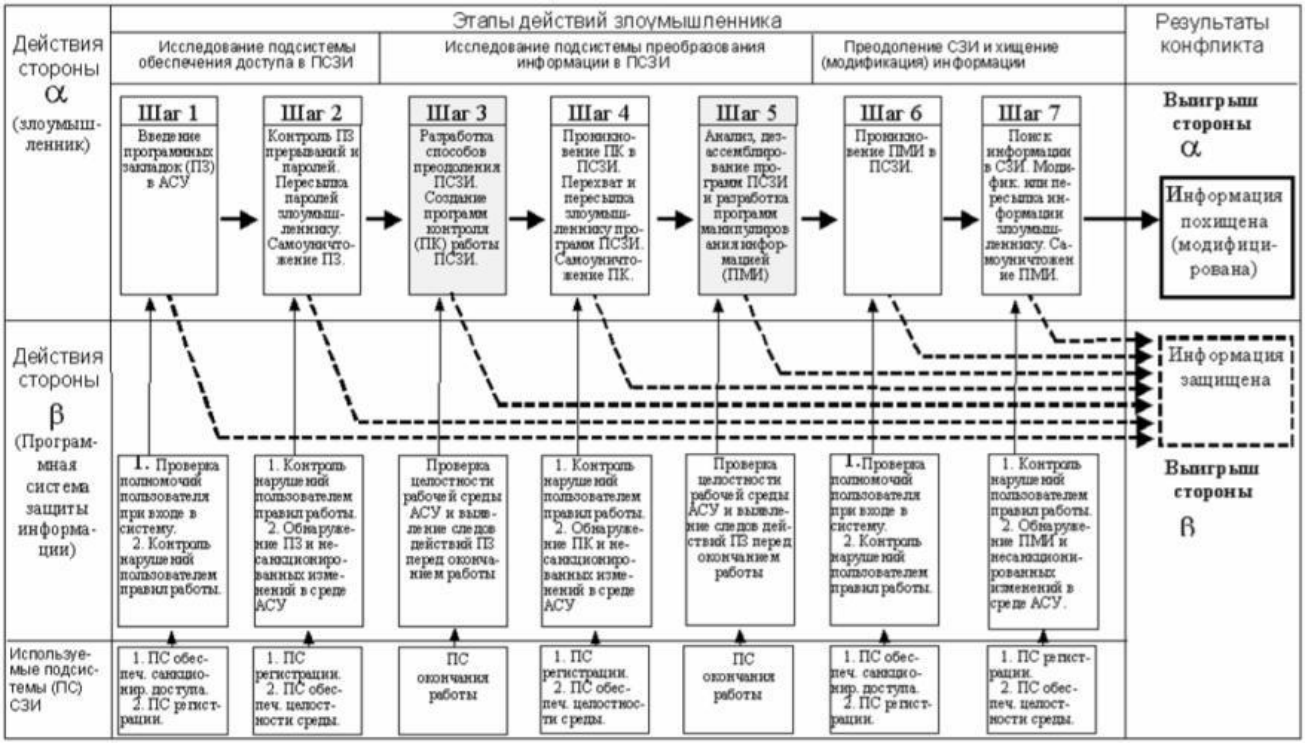


Рисунок 1.10 – Концептуальна модель конфлікту інформаційна система – джерело негативного впливу [21]

Етапи негативного цілеспрямованого впливу джерела негативного впливу на інформаційну систему представлено станами даного процесу [21]:

S_0 – початковий стан процесу;

S_1, S_2 … S_6 – проміжні стани процесу, які означають успішне виконання джерелом негативного впливу кроків, необхідних для того, щоб отримати доступ до інформації;

S_7 – кінцевий стан процесу, який означає, що сторона α виграла. Іншими словами, джерело негативного впливу отримало та модифікувало інформацію;

S_8 – кінцевий стан процесу, який означає, що сторона β виграла. Тобто, інформацію вдалося захистити;

Густина ймовірності відповідає за переходи між станами: $\omega_{01}(t), \omega_{12}(t), \omega_{23}(t), \omega_{34}(t), \omega_{45}(t), \omega_{56}(t), \omega_{67}(t), \omega_{08}(t), \omega_{18}(t), \omega_{28}(t),$

$\omega_{38}(t), \omega_{48}(t), \omega_{58}(t), \omega_{68}(t)$ [10].

Після цього, відповідно до [21], для випадкового напівмарковських процесу вирішується система рівнянь за допомогою якої визначається ймовірності виграшу сторони α або β, які власне і будуть відповідати можливостям того, зможе або не зможе джерело негативного впливу модифікувати бажану інформацію.

Таким чином, за допомогою продемонстрованого підходу можна враховувати певні особливості джерела негативного впливу, які несуть додатковий негативний негативний на систему вплив. Однак даний підхід має недоліки, зокрема:

– не враховується динаміка вразливостей в інформаційній системі, а саме залежність можливого навмисного негативного впливу на систему від наявності у даній системі вразливостей;

– вибір даних етапів є недоречним для навмисного негативного впливу. Неможливо знайти де-небудь статистику або ж отримати її самостійно, для того, щоб була можливість провести оцінку щільності ймовірності переходів поміж станів процесу конфліктної взаємодії інформаційної системи з джерелом негативного впливу, описаної в [21], тому що і джерела негативного впливу і фахівці у галузі

комп’ютерної безпеки характеризують процес здійснення негативного навмисного впливу радикально іншим чином, що описано в [24];

– не враховується ряд подій після того, як джерело негативного впливу захоплює інформацію, а саме: ні відмови в обслуговуванні, ні кількість атак, ні можливість інформаційної системи бути відновленою шляхом застосування резервної копії.

Отже, на сьогоднішній день можна виділити дві категорії підходів до аналізу надійності інформаційних технологій та систем в умовах конфліктних взаємодій, тобто з наявними вразливостями та джерелами негавтиного впливу – статичні та динамічні. Очевидно, що хоча динамічні підходи і дають кращий результат ніж статичні, але все таки мають певні недоліки, через які неможливе врахування найбільш важливих та значущих факторів, які можуть значно впливати на надійність інформаційної системи.

Тому можна визначити основні вимоги щодо розробки алгоритмів та моделей аналізу надійності інформаційних технологій та систем за умов конфліктної взаємодії, при наявних внутрішніх вразливостях системи та джерела негативного впливу:

– врахування характеру чинників, який зазвичай є випадковим, що впливає на надійність інформаційних технологій та систем;

– врахування динаміки конфлікту між різними суб’єктами, що беруть участь в цих процесах;

– врахування динаміки окремих процесів, що впливають на надійність інформаційних технологій та систем;

– реалізація алгоритмів та моделей, прогнозування даних;

– доступність джерел даних для оцінки параметрів, що впливають на надійність інформаційних технологій та систем;

– удосконалення алгоритмів та моделей шляхом використання принципів об'єктно-орієнтованого підходу, при якому не потрібно буде вносити серйозні зміни до досліджуваної загальної схеми.

2 ПОСТАНОВКА ЗАДАЧІ ТА МЕТОДИ ДОСЛІДЖЕННЯ

2.1 Мета та задачі дослідження

Основна мета даної роботи – поліпшення та оптимізація існуючої моделі аналізу надійності використання програмних технологій в інформаційних системах за умов конфлікту з джерелом негативного впливу шляхом розширення можливих варіацій ймовірнісних характеристик, а саме: наявність засобів захисту інформації, наявність одного чи коаліції джерел негативного впливу, взаємодія з інсайдером.

У ході виконання проекту необхідно розробити та удосконалити математичні та об’єктно-орієнтовані моделі, які будуть включати нові, важливі ймовірнісні характеристики можливого негативного впливу, що перераховані вище. На базі нових моделей будуть створені імітаційні моделі динаміки конфліктної взаємодії.

Для того, щоб дана робота вважалася виконаною, є необхідним вирішення наступних задач:

– аналіз сучасних підходів щодо оцінки надійності експлуатації програмного забезпечення в інформаційних системах на предмет урахування ряду вимог та факторів;

– аналіз ряду важливих чинників, що впливають на надійність експлуатації програм в інформаційних технологіях;

– формування основних вимог до алгоритмів і моделей аналізу надійності експлуатації програмного забезпечення в інформаційних системах, що будуть розроблюватися;

– розробка математичних, об’єктно-орієнтованих та відповідно імітаційних моделей аналізу надійності експлуатації програмного забезпечення в інформаційних системах за умов конфліктної взаємодії, які враховують нові важливі фактори можливого впливу на систему.

2.2 Методи дослідження

При вирішенні поставлених задач будуть використані наступні методи: апарат математичної статистики та теорії ймовірностей, математичний апарат марківських ланцюгів, а також технології комп’ютерного імітаційного моделювання.

Для розробки математичних моделей аналізу надійності використання програмного забезпечення інформаційних систем за умов конфліктної взаємодії, зручно представити моделі як марківський ланцюг з неперервним часом.

Під час переходу системи з одного стану в інший, обставини потравляння в цей стан системою враховуватися не повинні. А тому пропонується використовувати ймовірності переходів між станами, щоб описувати появу випадкових подій.

Марківським процесом називаємо випадковий процес, у якому ймовірність будь-якого стану системи в майбутньому для кожного моменту часу t залежить тільки від її стану в сьогоденні і не залежить від того, як система потрапила в цей стан.

Отже, марківский процес зручно задавати за допомогою графу з переходами зі стану в стан.

Час між переходами з одного стану в інший для процесів, що відбуваються випадково, та мають безперервний час, є випадковою величиною. Оскільки ймовірність такого переходу точно в довільний момент часу t дорівнює нулю, це означає, що ймовірність переходу з одного стану в інший не може бути заданим значенням. Тому вводиться деякий параметр, який називається інтенсивністю переходу, для того, щоб описувати переходи між станами випадкового процесу з безперервним часом замість ймовірностей переходів. Відповідно, марківським буде той випадковий процес з безперервним часом, у якому інтервали часу між сусідніми переходами зі стану в стан були розподілені за експоненціальним законом.

Аналіз вимог, яким мають задовольняти системи є початковим етапом при проектуванні прикладних програмних систем.

Цей аналіз необхідний для того, щоб зуміти скласти попередній проект системи, мати можливість дуже детально розібрати та зрозуміти умови експлуатації та призначення системи. Використовуючи об'єктно-орієнтований підхід, аналіз вимог системи можна звести до розробки моделей цієї системи. Модель системи або будь-якого іншого об'єкта, явища представляємо за допомогою формального опису системи, в якому виділяємо основні об'єкти, які складають систему, та взаємозв'язки між цими об'єктами. Побудова моделей – широко поширений спосіб вивчення складних об'єктів і явищ. У моделі опущені численні деталі, які ускладнюють розуміння. Для побудови об'єктно-орієнтованих моделей конфліктної взаємодії інформаційної системи та джерела негативного впливу будемо використовувати апарат мови UML.

Ускладнення формулювання завдання і необхідність врахування всіх значущих для опису інформаційного конфлікту чинників неминуче ведуть до зростаючих труднощів при використанні аналітичних математичних моделей. Це визначає істотну роль засобів і комп'ютерних технологій об'єктно-орієнтованого моделювання для дослідження закономірностей конфлікту.

Імітаційним моделюванням називається метод, за допомогою якого можлива побудова моделей, які можуть описувати процеси та дії, поведінку максимально наближено до реальності. До того ж створена модель може бути запущена та «програна» у часі не лише для одного випробування, а для безлічі можливих варіантів. При цьому отримані результати визначаються випадковим характером процесів. Використовуючи отримані дані можна формувати та отримувати достатньо стійкі статистичні результати. Тому і буде використаний даний метод дослідження, мета якого – отримання інформації про справжню систему шляхом заміни системи, що аналізується, моделлю, яка зможе досить точно описати справжню, та проводити з неї цикл експериментів. Імітацією називається експериментування з моделлю.

2.3 Вибір засобів реалізації

Для того щоб вирішити поставлені у роботі завдання, було використано апарат теорії ймовірностей і математичної статистики, математичний апарат марківських ланцюгів, а також технології комп’ютерного імітаційоного моделювання.

При моделюванні інформаційних систем і технологій будуть використані наступні види моделей: математичні моделі, побудовані на використанні імовірнісних описах динаміки конфліктної взаємодії, об’єктно-орієнтовані моделі в нотаціях UML, та імітаційні моделі, які реалізовані в середовищі Matlab з бібліотеками Simulink та Stateflow, що забезпечить найбільш повне та корректне врахування вихідних функціональних та концептуальних об'єктних представлень.

Під час планування робіт будуть використані наступні інструменти: для побудови діаграми Ганта використаний онлайн ресурс GanttPRO, що дозволяє якісно та швидко створити наочний план проекту та має інтуїтивно зрозумілий, зручний, дружній до користувача інтерфейс[25]. Для мережевого графіка та різних схем використано онлайн ресурс Draw.io, бо це сервіс, який якраз і призначений для формування діаграм і схем. За допомогою даного онлайн сервісу також можна розробляти діаграми, моделі, блок-схеми, графіки, форми тощо [26].

Тому саме цей інструмент було обрано для формування мережевого графіка та марківської моделі конфліктної взаємодії інформаційної системи із джерелом негативного впливу, тому що містить весь необхідний набір інструментів, таких як фігури, написи. Стрілки тощо для якісної демонстрації. Має інтуїтивно зрозумілий інтерфейс, розширений функціонал, зручний у використанні редактор.

Розробка UML діаграм проводиться з використанням середовища Visual Studio 2015 так як підтримує спеціальний набір інструментів для розроблення діаграмм такого роду. Можливості у повному обсязі забезпечують, якісну роботу та розробку діаграм.

Реалізація імітаційних моделей відбувається у Matlab-середовищі, використовуючи вбудовані бібліотеки Simulink та Stateflow.

Matlab - це середовище і мова технічних розрахунків, призначений для вирішення широкого спектра інженерних і наукових завдань будь-якої складності в будь-яких галузях. Це одночасно мова інженерних розрахунків, додатки з графічним інтерфейсом, засоби розробки програмного забезпечення, більше сотні прикладних програм та професійних розширень системи та її адаптації під рішення певних класів математичних і науково-технічних завдань.

Simulink – середовище динамічного моделювання складних технічних систем і основний інструмент для модельно-орієнтованого проектування. Його основним інтерфейсом є графічний інструмент для побудови діаграм і настроюється набір бібліотек блоків. Він пропонує тісну інтеграцію з рештою середовищ Matlab і може або використовувати Matlab, або створювати сценарії з нього. Simulink широко використовується в автоматичному управлінні та проектування на основі моделей. У поєднанні з іншими своїми продуктами Simulink може автоматично генерувати вихідний код на мові C для реалізації систем в режимі реального часу [27-28].

Stateflow надає графічну мову, яка включає діаграми переходів станів, блок-схеми, таблиці переходів станів і таблиці істинності. Stateflow використовується, щоб описати, як алгоритми Matlab і моделі Simulink реагують на вхідні сигнали, події і умови на основі часу. Stateflow дозволяє проектувати і розробляти диспетчерське управління, планування завдань, управління відмовами, протоколами зв'язку, призначені для користувача інтерфейси і гібридні системи. За допомогою Stateflow створюється комбінаторна логіка і логіка прийняття рішень, які можна змоделювати як блок в моделі Simulink або виконати як об'єкт в Matlab. Графічна анімація дозволяє аналізувати і налагоджувати свою логіку під час її виконання. В той час перевірки під час редагування та під час виконання забезпечують узгодженість і повноту проектування перед впровадженням [28-29].

3 РОЗРОБКА МАТЕМАТИЧНИХ ТА ОБ'ЄКТНО-ОРІЄНТОВАНИХ МОДЕЛЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ КОНФЛІКТНИХ ВЗАЄМОДІЙ

3.1 Проектування процесу розробки інформаційної технології

Найпершим кроком необхідним при створенні інформаційної технології є розуміння, як саме має працювати те, що збираються автоматизувати. Для описання даної роботи є необхідною побудова загальної моделі. Ця модель має бути адекватною до предметної області, та в ній мають розміщуватися знання всіх, хто бере участь у бізнес-процесах даної організації.

IDEF0 є однією з найзручніших мов моделювання бізнес-процесів. Система у даній методології представлена сукупністю взаємодіючих та взаємозв'язаних функцій чи робіт. Основною є лише функціональна направляюча методології, тому що аналіз функціонування системи не залежить від об'єктів, якими вони оперують, що дає право адекватно та якісно моделювати логіку та взаємодію організаційних процесів [30].

Для початку процесу моделювання системи в даній методології, визначається найбільш абстрактний рівень описування системи загалом, тобто іншими словами – контекст. До контексту входить визначення мети, і точки зору на модель, а також суб'єкта моделювання. Під суб'єктом необхідно розуміти саму систему. До того ж є необхідним точне встановлення того, які компоненти входять до системи, а які – лежать за її межею. Тобто, необхідно сформулювати, що буде розглянуто як складові системи в подальшому, а що – як зовнішній вплив на неї. На характеризування суб'єкта системи суттєво впливає позиція, з якої точки зору розглядається система та ціль моделювання – запитання, на яке має відповідати побудована модель. Тобто, насамперед, треба визначитися з областю моделюваня. Описування області як в єдиної системи, так і її складових частин є головним у побудові моделі. Попри те, що, очевидно, область може буде виправлена, підкоригована, в основному вона має бути

сформульована с самого спочатку, тому що саме за допомогою області визначається напрямок моделювання, і коли модель вже є готовою і має бути закінчена [30]. Тому було визначено предметну область даного проекту: інформаційні технології, а точка зору – студент та керівник.

Без чітко сформульованої мети модель не може бути побудована, бо формулювання мети дозволяє команді аналітиків сфокусувати зусилля в потрібному напрямку. Тому для даного проекту була визначена мета: розробити інформаційну технологію аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів яка дозволяє врахувати динаміку зміни вразливостей, а також ряд інших параметрів, що визначають ситуаційний характер конфліктної взаємодії сторін.

Графічна мова опису бізнес-процесів є основою методології IDEF0, а тому модель представляє собою сукупність взаємопов’язаних та ієрархічно впорядкованих діаграм в даній нотації. Кожна така діаграма – це одиниця опису системи та має розташовуватися на окремомих аркушах.

Дана діаграма складається з чотирьох блоків, так як однією з вимог IDEF0 є, щоб діаграма містила не більше, ніж шість, але при цьому не менше, ніж три блоки. Дані обмеження необхідні для підтримки складності діаграм та моделей на рівні, що доступний для розуміння, читання та використання.

Блоки розміщені за ступенем важливості. Розміщення з відносним порядком називається домінуванням. Це дозволяє продемонструвати, як один блок діаграми впливає на інші. Найдомінуючішим блоком з заданої послідовності функцій діаграми завжди виступає перший блок. Блок, що домінує найбільше у даній схемі знаходиться у лівому верхньому кутку діаграми, відповідно у правому нижньому кутку знаходиться блок, що домінує найменш всього.

Представлена на рисунку 3.1 контекстна діаграма, демонструє навколишні взаємодії із процесами, коротку інформацію про предметну області, мету та точки зору.

Для того, щоб даний процес був розпочатий, треба мати конкретно задану мету, яким чином і що саме має бути отримано на виході. Це надасть можливість

моделювати нові та покращувати існуючі математичні, об’єктно-орієнтовані моделі та власне імітаційні моделі.

Даний процес контролювати має науковий керівник, та технічне завдання, згідно з яким все має бути виконано. Як результат, у кінці мають бути отримані наступні результати:

- математична модель з засобами захисту інформації;
- об'єктно-орієнтована модель конфлікту з засобами захисту інформації;
- імітаційна модель конфлікту з засобами захисту інформації;
- математична модель конфлікту з інсайдером;
- об'єктно-орієнтована модель конфлікту з інсайдером;
- імітаційна модель конфлікту з інсайдером;
- математична модель конфлікту з коаліцією джерел негативного впливу;
- об'єктно-орієнтована модель конфлікту з коаліцією джерел негативного впливу;
- імітаційна модель конфлікту з коаліцією джерел негатвиного впливу.

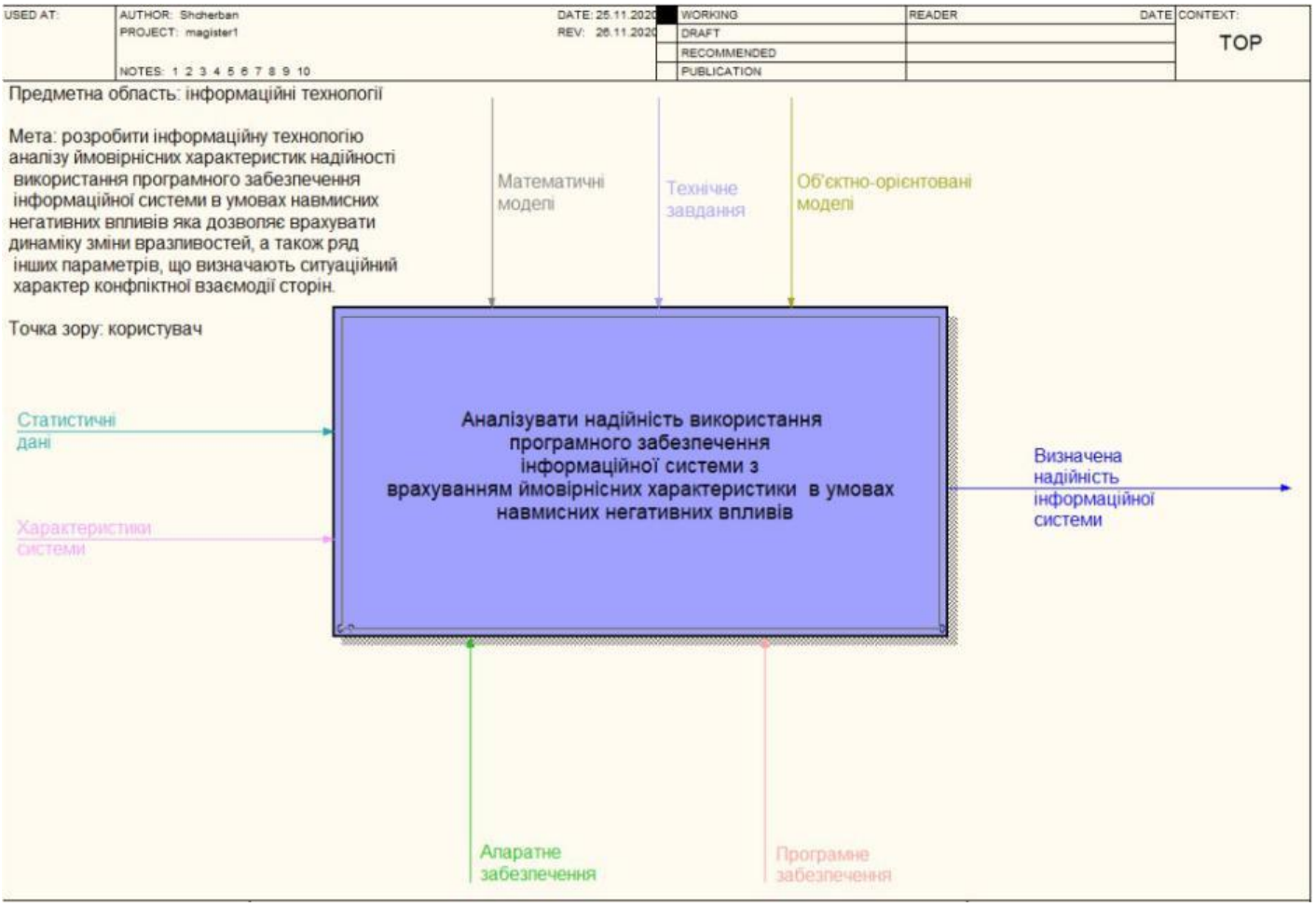


Рисунок 3.1 – Контекстна діаграма IDEF0

Була проведена декомпозиція діаграми на один рівень. Для того, щоб був виконаний процес, нам перш за все є необхідною розробка математичних моделей конфлікту інформаційної системи з рядом ймовірнісних характеристик конфлікту. Цей процес має бути проконтрольований керівником та виконаний згідно з технічним завданням. Має бути використане необхідне програмне та апаратне забезпечення, а також з дотриманням усіх правил теорії напівмарківських процесів. Після виконання даної дії будуть отримані математичні моделі.

На їх базі вже є можливість проектувати об’єктно-орієнтовані моделі. Якщо виникають помилки або неузгодження, то можливо необхідно переглянути математичні моделі. Даний процес також має бути проконтрольований керівником та виконаний згідно з технічним завданням.

Наступним кроком є проектування імітаційні моделі. У випадку виникнення проблем під час проектування імітаційних моделей, важливо перевірити корректність об’єктно-орієнтованих моделей. Після проведення імітацій необхідно їх проаналізувати й перевірити отримані результати, які отримали з використанням імітаційної моделі. Отсаннім процесом будет побудова графіку з результатом надійності системи. На рисунку 3.2 представлена декомпозована діаграма з описаними вище процесами.

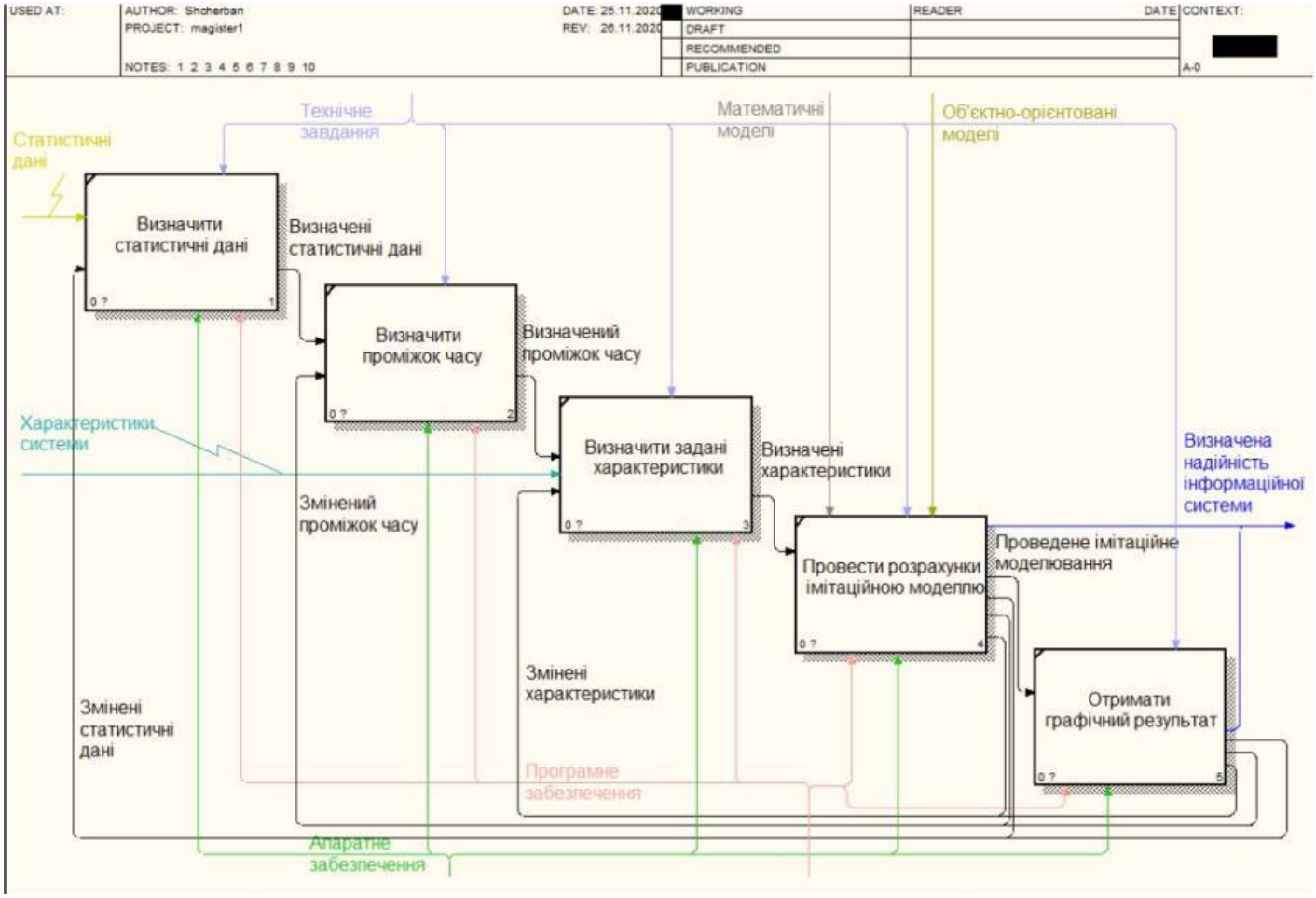


Рисунок 3.2 – Декомпозиція діаграми IDEF0

Завдяки створенню даних діаграм, є наочна можливість побачити послідовність та пріорітетність виконання дій, а також отримані результати, та визначити можливі елементи контролю та необхідне обладнання.

3.2 Математична модель конфлікту інформаційної системи з відсутніми засобами захисту інформації і одним джерелом негативного впливу

Математична модель конфліктної взаємодії інформаційної системи з відсутніми засобами захисту інформації та джерела негативного впливу ґрунтується на поданні процесів зміни станів в об'єднаній системі інформаційна сиситема – джерело негативного впливу у вигляді марківського ланцюга з кінцевою кількістю станів, переходи між якими відбуваються за пуассонівським, тобто експоненціальним, законом розподілу [31]. Описана модель представляє собою розширення найпростішої математичної моделі конфлікту інформаційної системи та джерела негативного впливу, а саме характеристику можливої поведінки джерела негативного впливу залежно від кваліфікації та досвіду. Нижче на рисунку 3.3 продемонстровані стани, у яких джерело негативного може знаходитится під час підготовки та здійсненні негавтиного впливу на інформаційну систему, та усі можливі переходи між цими станами.

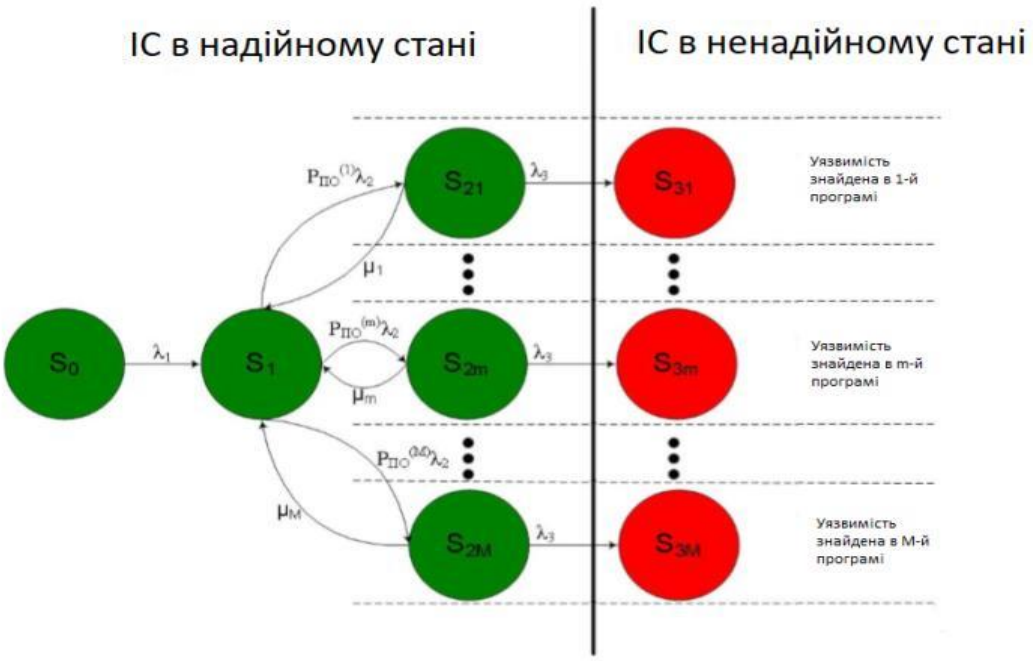


Рисунок 3.3 – Математична модель конфлікту інформаційної системи з відсутніми засобами захисту інформації і джерелом негативного впливу

Стани характеризуються відповідними наступними вузлами ланцюга:

S_0 – будь-яка інформація про інформаційну систему у джерела негативного впливу відсутня (стан «Немає інформації щодо інформаційної системи» в об'єктно-орієнтованій моделі);

S_1 – є інформація щодо програмного забезпечення інформаційної системи у джерела негативного впливу (стан «Інформація про програмне забезпечення інформаційної системи» в об'єктно-орієнтованій моделі);

S_{2m} – джерело негативного впливу має інформацію про програмне забезпечення інформаційної системи і про одну вразливість в цьому програмному забезпеченні, де m – номер програмного додатку, в якому була виявлена вразливість ($m \in 1..M$), а M – число програм в інформаційній системі (стан «Інформація про вразливості в програмне забезпечення інформаційної системи» в об'єктно-орієнтованій моделі);

S_{3m} ($m \in 1..M$) – у джерела негативного впливу є інформація про програмне забезпечення інформаційної системи, про одну вразливість в цьому програмному забезпеченні, а також про спосіб, як використати цю вразливість для здійснення негативного впливу на інформаційну систему (стан «Інформація про спосіб використання вразливості для негативного впливу на інформаційну систему» в об'єктно-орієнтованій моделі).

Імовірності перебування в перерахованих станах будемо позначати відповідно $P_0, P_1, P_{21}, \ldots P_{2m}, \ldots P_{2M}, \ldots, P_{31}, \ldots P_{3m}, \ldots . P_{3M}$. У той же час, частина зазначених станів агрегується в стан «Інформаційна система в надійному стані», що відповідає стану «Надійний стан» в об'єктно-орієнтованій моделі, а стани ($S_{31}, \ldots S_{3m}, \ldots S_{3M}$) – в стан «Інформаційна система в ненадійному стані», що відповідає стану «Ненадійний стан» в об'єктно- орієнтованій моделі.

Інтенсивність переходу із S_0 стану в S_1 відбувається за:

$$\lambda_1 = \frac{1}{T_{no}}, \tag{3.1}$$

де T_{no} – середній час, потрібний джерелу негативного впливу для знаходження інформації про програмне забезпечення інформаційної системи.

Зміна станів S_1 в стани S_{2m} $(m \in 1..M)$ відбуваються з інтенсивностями $P_{\text{ПЗ}}^{(m)}\lambda_2$, де $P_{\text{ПЗ}}^{(m)}$ – пошуку інформації про вразливість в m-ому програмному забезпечені, що рівняється:

$$P_{\text{ПЗ}}^{(m)} = \frac{N_{\text{ср\_конф}}^{(m)}}{N_{\text{ср\_конф}}} \tag{3.2}$$

де $N_{\text{ср\_конф}}^{(m)}$ – середнє арифметичне середньостатистичного числа вразливостей, що знаходяться у m-му програмному додатку в інформаційній системі, $N_{\text{ср}}^{(m)}(t)$, а $N_{\text{ср\_конф}}$ – середнє арифметичне середньостатистичного усіх вразливостей, які знаходяться в програмному забезпеченні інформаційної системи $N_{\text{ср}}(t)$.

Інтенсивність знаходження вразливостей в програмному забезпеченні інформаційної системи:

$$\lambda_2 = \frac{N_{\text{ср\_конф}}}{T_{\text{вразл}}} \tag{3.3}$$

де $T_{\text{вразл}}$ – середній час, який необхідний джерелу негативного впливу для пошуку інформації про всі вразливі сторони в інфомаційній системі. З урахуванням (3.2) і (3.3) інтенсивності зміни станів з S_1 на S_{2m} $(m \in 1..M)$ будуть становити:

$$P_{\text{ПЗ}}^{(m)}\lambda_2 = \frac{N_{\text{ср\_конф}}^{(m)}}{T_{\text{вразл}}} \tag{3.4}$$

Зміна стану $S_{2m}(m \in 1..M)$ в стан S_{3m} $(m \in 1..M)$ відбувається з наступною інтенсивністю:

$$\lambda_3 = \frac{1}{T_{\text{нв}}}, \tag{3.5}$$

де $T_{\text{нв}}$ – середній час, що необхідний джерелу негативного впливу для пошуку даних про спосіб користування вразливостями в програмному забезпеченні для негативного впливу на інформаційну систему.

Для знаходження середнього часу, з моменту пошуку джерела негативного впливу вразливості до її виключення з інформаційної системи, будуть оптимальними наступні міркування. Допускається, що час виявлення вразливості в m-й програмному забезпечені $T^{(m)}_{\text{обн\_вразл}}$ є випадковою величиною, що отримує з постійною імовірністю значення з проміжку від різниці поточного $\text{T}_{\text{тек}}$ і середнього часів існування дефекту в m-й програмному забезпеченні $T^{(m)}_{\text{жизн\_вразл}}$ до поточного часу $\text{T}_{\text{тек}}$, отже, її математичне сподівання рівняється $\text{T}_{\text{тек}} = \frac{\text{T}^{(m)}_{\text{жизн\_вразл}}}{2}$, а час з початку пошуку джерелом негативного впливу даних про дефекти в m-й програмнму забезпеченні до закриття $T^{(m)}_{\text{закр}}$ цього дефекту відповідно рівняється:

$$T^{(m)}_{\text{закр}} = \frac{\text{T}^{(m)}_{\text{жизн\_вразл}}}{2} \tag{3.6}$$

Середню тривалість життя вразливості в m-й програмному забезпеченні можна розрахувати за формулою:

$$T^{(m)}_{\text{жизн\_вразл}} = \frac{\text{T}^{(m)}_{\text{в}}}{k^{(m)}}, \tag{3.7}$$

де $\text{T}^{(m)}_{\text{в}}$ – час, що необхідно для вендора m-ї програмного забезпечення для створення патча та або непостійного рішення, яке закриває вразливість, з моменту її знаходження, $k^{(m)}$ – – коефіцієнт відображення роботи системного адміністратора задля вирішення вразливостей з m-ого програмного забезпечення.

Зміна стану $S_{2m}(m \in 1..M)$ в $S_{3m}(m \in 1..M)$ відбувається з використанням інтенсивностей:

$$\mu_m = \frac{1}{T_{\text{закр}}^{(m)}}, \tag{3.8}$$

Які зважаючи на 3.6 і 3.7 дорівнюють:

$$\mu_m = \frac{2k^{(m)}}{T_{\text{в}}^{(m)}}, \tag{3.9}$$

Згідно з [14,29] отриманий ланцюг Маркова описується вектором початкового розподілу вірогідності знаходження в різних станах:

$$P(0) = [1\ 0\ \ldots\ 0]\ , \tag{3.10}$$

і перехідною матрицею, яка з урахуванням (3.1), (3.4), (3.5) і (3.9) набуває вигляду:

$$P_{пер}(t) = \exp(Qt),$$

$$Q = \begin{bmatrix} 1-\frac{1}{T_{по}} & \frac{1}{T_{по}} & 0 & \ldots & 0 & 0 & .. & 0 \\ 0 & 1-\sum_{m=1}^{M}\frac{N_{ср\_конф}^{(m)}}{T_{уязв}} & \frac{N_{ср\_конф}^{(1)}}{T_{уязв}} & \ldots & \frac{N_{ср\_конф}^{(M)}}{T_{уязв}} & 0 & \ldots & 0 \\ 0 & \frac{2k^{(1)}}{T_{в}^{(1)}} & 1-\left(\frac{2k^{(1)}}{T_{в}^{(1)}}+\frac{1}{T_{нв}}\right) & \ldots & 0 & \frac{1}{T_{нв}} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \frac{2k^{(M)}}{T_{в}^{(M)}} & 0 & \ldots & 1-\left(\frac{2k^{(M)}}{T_{в}^{(M)}}+\frac{1}{T_{нв}}\right) & 0 & \ldots & \frac{1}{T_{нв}} \\ 0 & 0 & 0 & \ldots & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & .. & 1 \end{bmatrix}. \tag{3.11}$$

де Q – матриця інтенсивностей переходів з одного стану в інший; t – час, що рахується з самого почтаку конфліктної взаємодії.

Розподіл ймовірностей в момент часу t с початку конфлікту розраховується згідно з [14] за такою формулою:

$$P(t) = P(0)P_{\text{пер}}(t), \tag{3.12}$$

Ймовірність знаходження інформаційної системи в надійному стані на n-му кроці конфлікту буде дорівнювати:

$$P_{\text{нах\_над}}\ (t) = 1 - \sum_{m=1}^{M} P_{3m}(t) \tag{3.13}$$

Ймовірність знаходження інформаційної системи в надійному стані за весь час конфлікту буде дорівнює середньому арифметичному між вірогідністю знаходження інформаційної системи в надійному стані на кожному кроці конфлікту:

$$P_{нах\_над\_конф} = \frac{\int_0^{T_{конф}} P_{нах\_над}(t)dt}{T_{конф}}, \tag{3.14}$$

де $T_{конф}$ – час тривалості конфлікту. З урахуванням (3.12-3.13) формула (3.14) приймає вигляд:

$$P_{нах\_над\_конф} = \frac{\int_0^{T_{конф}} \left(1 - \sum_{m=1}^{M} \left(P(0)P_{пер}(t)\right)_{3m}\right)dt}{T_{конф}}. \tag{3.15}$$

Ймовірність влучення інформаційної системи в ненадійний стан протягом часу конфлікту буде розраховуватися як:

$$P_{\text{ненад}} = \sum_{m=1}^{\text{M}} P_{3m}(T_{\text{конф}}), \quad (3.16)$$

а ймовірність надійності інформаційної системи, тобто ймовірність непотрапляння в ненадійний стан протягом часу конфлікту, відповідно рівний:

$$P_{\text{над}} = 1 - \sum_{m=1}^{\text{M}} P_{3m}\left(T_{\text{конф}}\right), \quad (3.17)$$

а з врахуванням 3.12:

$$P_{\text{над}} = 1 - \sum_{m=1}^{\text{M}} (P(0)P_{\text{пер}}\left(T_{\text{конф}}\right))_{3m}. \quad (3.18)$$

3.3 Математична модель функціонування інформаційної системи з засобами захисту інформації в умовах конфліктних взаємодій з одним джерелом негативного впливу

Для того, щоб математична модель конфлікту інформаційної системи і одного джерела негативного впливу враховувала наявний в інформаційній системі засіб захисту інформації, в ній необхідно застосувати певні зміни, а саме додати стани, що відображають розвідку інформації про засоби захисту інформації інформаційної системи для негативного впливу на ці засоби захисту інформації, а також переходи в стани, відповідні наявності інформації про засоби захисту інформації з усіх наступних станів. Дана математична модель з внесеними змінами зображена на рисунку 3.4.

Рисунок 3.4 – Математична модель конфлікту системи з засобом захисту інформації та одного джерела негативного впливу

Інтенсивність переходу із стану S_0 в стан S_1:

$$v_1 = \frac{1}{T_{\text{ззі}}}, \tag{3.19}$$

де $T_{\text{ззі}}$ – середній час, необхідний джерелу негативного впливу для знаходження інформації про засоби захисту інформації інформаційної системи.

Інтенсивність переходу із стану S_1 в стан S_2:

$$v_2 = \frac{N_{\text{ср\_конф}}^{(\text{ззі})}}{\text{Т}_{\text{вразл\_ззі}}}, \tag{3.20}$$

де $\text{Т}_{\text{вразл\_ззі}}$ – середній час, необхідний джерелу негативного впливу для знаходження інформації про одну вразливість у засобу захисту інформації, а $N_{\text{ср\_конф}}^{(\text{ззі})}$ – середнє арифметичне середньої статистичної кількості вразливостей $N^{(\text{ззі})}(t)$, що знаходяться в засобах захисту інформації за час розгляду конфлікту.

Інтенсивність переходу із стану S_2 в стан S_3:

$$v_3 = \frac{1}{T_{\text{нв\_ззі}}}, \tag{3.21}$$

де $T_{\text{нв\_ззі}}$ – середній час, необхідний джерелу негативного впливу для знаходження інформації про способи вразливостей в засобах захисту інформації для негативного впливу на них.

Інтенсивність переходу із станів S_2, S_3, S_4, $S_{5m}(m \in 1..M)$, $S_{6m}(m \in 1..M)$ в стан S_1 виводиться наступним чином:

$$\mu_{\text{ззі}} = \frac{2k_{\text{закр}}^{(\text{ЗЗІ})}}{T_{\text{в}}^{(\text{ЗЗІ})}}\text{,,} \tag{3.22}$$

Де $T_{\text{в}}^{(\text{ЗЗІ})}$ – час, який необхідний вендору засобів захисту інформації для сворення патчу або тимчасового рішення, що закриває вразливість в засобах захисту інформації з моменту її виявлення, а $k_{\text{закр}}^{(\text{ЗЗІ})}$ – коефіцієнт, що відображає роботу системного адміністратора щодо усунення вразливостей із засобу захисту інформації. Всі інші інтенсивності переходів визначаються так само, як і в математичній моделі конфлікту інформаційної системи з відсутніми засобами захисту інформації[12,13].

Отриманий марківський ланцюг при вирішенні описується вектором початкового розподілу вірогідності знаходження в різних станах P(0) = [1 0 0 .. 0] і перехідною матрицею, що розраховується подібно уже визначеному випадку конфлікту системи без засобів захисту з джерелом негативного впливу.

Аналогічним чином розраховується час знаходження системи в надійному стані:

$$P_{нах\_над\_конф} = \frac{\int_0^{T_{конф}} \left(1 - \sum_{m=1}^{M} \left(P(0)P_{пер}(t)\right)_{3m}\right) dt}{T_{конф}}. \tag{3.23}$$

Ймовірність надійності інформаційної системи у даному випадку дорівнює:

$$P_{\text{над}} = 1 - \sum_{m=1}^{\text{M}}(P(0)P_{\text{пер}}(T_{\text{конф}}))_{6m}. \quad (3.24)$$

3.4 Математична модель функціонування інформаційної системи в умовах конфліктних взаємодії із коаліцією джерел негативного впливу без інсайдера

Математична модель конфлікту інформаційної системи з коаліцією джерел негативного впливу аналогічна моделі конфлікту інформаційної системи з одним джерелом негативного впливу. При цьому інтенсивності переходів $\lambda_1, \lambda_2, \lambda_3$, що описують послідовне добування інформації про програмне забезпечення, про вразливості в ньому та про спосіб її використання для негативного впливу будемо розраховувати згідно з [14,15] як суми цих же інтенсивностей для кожного джерела негативного впливу $(\lambda_1^{(r)}, \lambda_2^{(r)}, \lambda_3^{(r)}, (r \in 1..R))$, які розраховувалися за допомогою формул:

$$\lambda_1 = \sum_r^R \lambda_1^{(r)},\ \lambda_2 = \sum_r^R \lambda_2^{(r)},\ \lambda_3 = \sum_r^R \lambda_3^{(r)} \quad (3.25)$$
$$\lambda_1 = \frac{1}{T_{\text{пз}}^{(r)}}, \lambda_2 = \frac{1}{T_{\text{вразл}}^{(r)}}, \lambda_3 = \frac{1}{T_{\text{нв\_ззі}}^{(r)}},$$

Де r – номер джерела негативного впливу, R – загальна кількість джерел, що входять в коаліцію, $T_{\text{вразл}}^{(r)}$- середній час, необхідний r-му джерелу для отримання інформації про всі вразливості в програмному забезпеченні, $T_{\text{пз}}^{(r)}$- середній час, необхідний r-му джерелу для отримання інформації про програмне забезпечення, $T_{\text{нв\_ззі}}^{(r)}$- середній час, необхідний r-му джерелу для отримання інформації про використання вразливості в програмному забезпечнні для негативного впливу.

3.5 Математична модель функціонування інформаційної системи в умовах конфліктних взаємодії із коаліцією джерел негативного впливу з інсайдером

Математична модель конфлікту інформаційної системи з коаліцією джерел негативного впливу аналогічна моделі конфлікту інформаційної системи з одним джерелом негативного впливу, але інтенсивності переходів λ_1, λ_2, що описують послідовне добування інформації про програмне забезпечення, про вразливості в ньому включають в себе також відповідні інтенсивності інсайдера ($\lambda_1^{(\text{інс})}, \lambda_2^{(\text{інс})}$[32,33].

$$\lambda_1 = \sum_r^R \lambda_1^{(r)} + \lambda_1^{(\text{інс})},\ \lambda_2 = \sum_r^R \lambda_2^{(r)} + \lambda_2^{(\text{інс})}, \qquad (3.26)$$
$$\lambda_1^{\text{інс}} = \frac{1}{T_{\text{пз}}^{(\text{інс})}},\ \lambda_2 = \frac{1}{T_{\text{вразл}}^{(\text{інс})}},$$

де $T_{\text{пз}}^{(\text{інс})}$- середній час, що необхідний інсайдеру для отримання інформації про програмне забезпечення, $T_{\text{вразл}}^{(\text{інс})}$- середній час, необхідний інсайдеру для отримання інформації про всі вразливості в програмних забезпеченнях.

3.6 Об’єктно-орієнтована модель функціонування інформаційної системи з відсутніми засобами захисту інформації в умовах конфліктних взаємодії із одним джерелом негативного впливу

Нехай існує інформаційна система в якій встановлено програмне забезпечення. Джерело негативного впливу, що скоює навмисний вплив на інформаційну систему, а саме, проводить попередній аналіз, тобто комп’ютерну розвідку щодо програмного забезпечення, що встановлене в інформаційній системі, в цьому програмному забезпеченні проводить дослідження вразливостей і можливих способів використання цих вразливостей [24]. При цьому джерело негативного впливу може

бути різної кваліфікації і з різними можливостями. Дані параметри джерела негативного впливу будемо визначати середнім часом, необхідним джерелу негативного впливу [34]: для отримання інформації про програмне забезпечення інформаційної системи; для отримання інформації про всі вразливі місця в програмному забезпеченні інформаційної системи; для отримання інформації про використання дефекту в програмному забезпеченні інформаційної системи для організації негативного впливу на інформаційну систему. При цьому динаміка вразливостей програмного забезпечення інформаційної системи може описуватися за допомогою найпростішої математичної моделлі інформаційної системи, що розглядалась раніше.

Для того, щоб побудувати об'єктно-орієнтовані моделі конфліктної взаємодії варто застусувати апарат мови UML [35], з використанням діаграми станів для опису поведінки сторін, що беруть участь в конфліктній взаємодії. На рисунках 3.5 – 3.7, що нижче, продемонстровано діаграмми станів, за допомогою яких описується поведінка інформаційної системи, джерела негативного впливу та системного адміністратора.

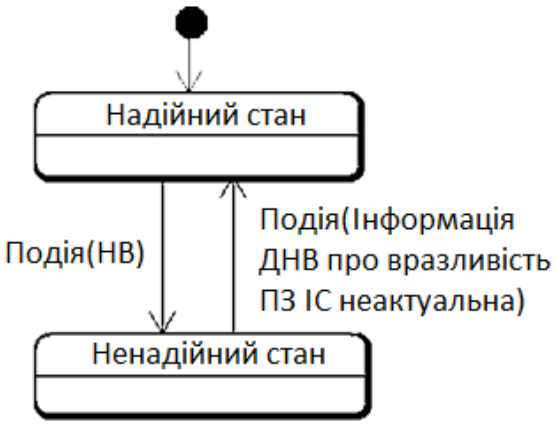


Рисунок 3.5 – Діаграма станів інформаційної системи з відсутніми засобами захисту інформації в ході конфліктної взаємодії із джерелом негативного впливу

Як продемонстровано на рисунку 2.5, в 2-х основних станах може перебувати інформаційна система:

– у стані «Надійний стан» – стан, коли успішний вплив на інформаційну систему джерелом негативного впливу не може бути здійснений;

– у стані «Ненадійний стан» – стан, коли успішний вплив на інформаційну систему джерелом негативного впливу може бути здійснений;

Передбачено момент, що спочатку інформаційна система перебуває у «надійному стані». Перехід з «Надійного стану» в «Ненадійний» здійснюється при події «негативний вплив». Зворотній перехід відбувається, коли генерується подія «неауктуальна інформація, яку знає джерело негативного впливу про вразливість в програмному забезпеченні інформаційної системи».

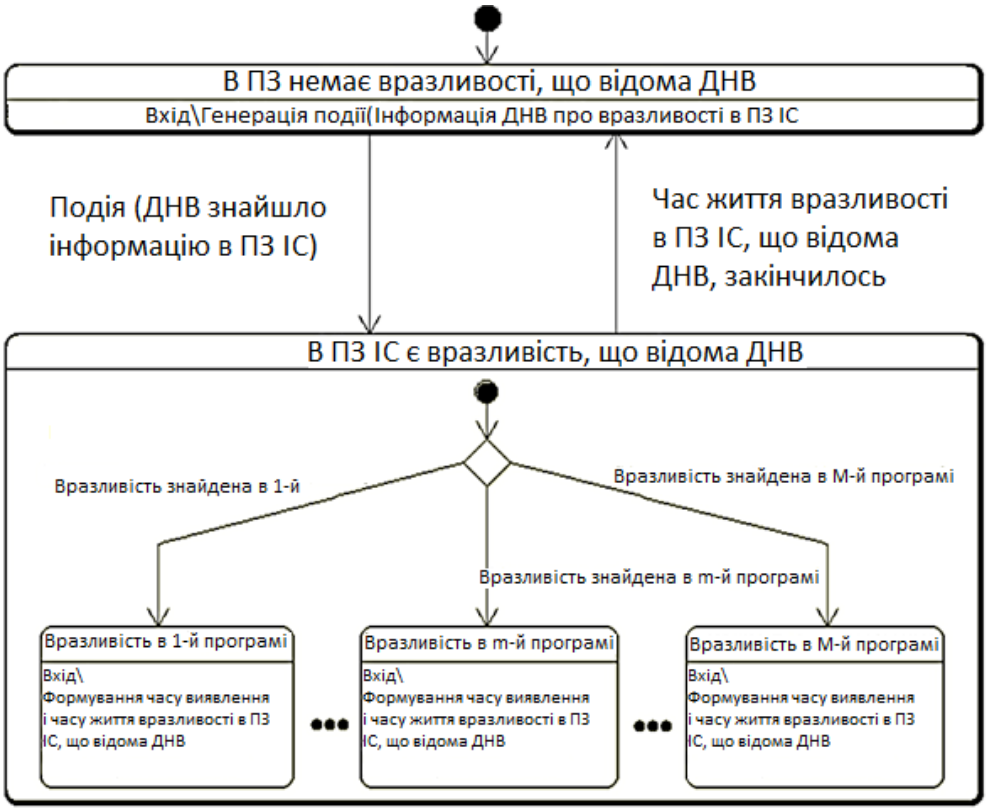


Рисунок 3.6 – Діаграма станів системного адміністратора під чам конфлікту інформаційної система з відсутніми засобами захисту інформації з джерелом негативного впливу

Можливі дії системного адміністратора представлені 2-ма станами, що на рисунку 3.6, тобто це стани, яка може мати дефект, відомий джерелу негативного впливу:

– стан «У програмного забезпечення інформаційної системи немає вразливості, відомої джерелу негативного впливу» – стан , при якому джерело негативного впливу не володіє інформацією про вразливість в програмному забезпеченні інформаційної системим ;

– стан «У програмне забезпечення інформаційної системи є вразливість, відома джерело негативного впливу» – стан, при якому у джерела негативного впливу є інформація про вразливість в прогамному забезпеченні інформаійної системи.

Передбачено момент, що системний адміністратор спочатку знаходиться в «У програмних додатках інформаційної системи відсутні вразливості, про які знає джерело негативного впливу» стані. При потраплянні в цей стан формується подія «Неактуальна інформація про дефект в програмному забезпеченні інформаційної системи, яку знає джерело негативного впливу». Перехід в «В програмному забезпеченні інформаційної системи є відомий джерелу негативного впливу дефект» стан відбувається при генерації події «Інформація про вразливість в програмному забезпеченні інформаційної системи знайдена джерелом негативного впливу». У цьому стані вибирається один з можливих підтсанів: «Вразливість в 1-му програмному додатку», ..., «Вразливість в 2-му програмному додатку», ..., «Вразливість в М-му програмному додатку» (всього в інформаційній системі встановлено М програмних додатків, $m \epsilon \overline{1, M}$). Залежно від того, в якому програмному додатку була виявлена відома джерелу негативного впливу вразливість, генерується час виявлення дефекту в обраному підстані і час його життя – тривалість до моменту випуску тимчасового рішення, а згодом і патча, що зможе усунути вразливість. Зворотний перехід в стан «У програмному забезпеченні інформаційної системи немає дефекту, що відомий джерелу негативного впливу» зі стану «У програмне забезпечення інформаційної системи є відомий джерелу негативного впливу дефект» відбувається за умови закінчення часу життя дефекту.

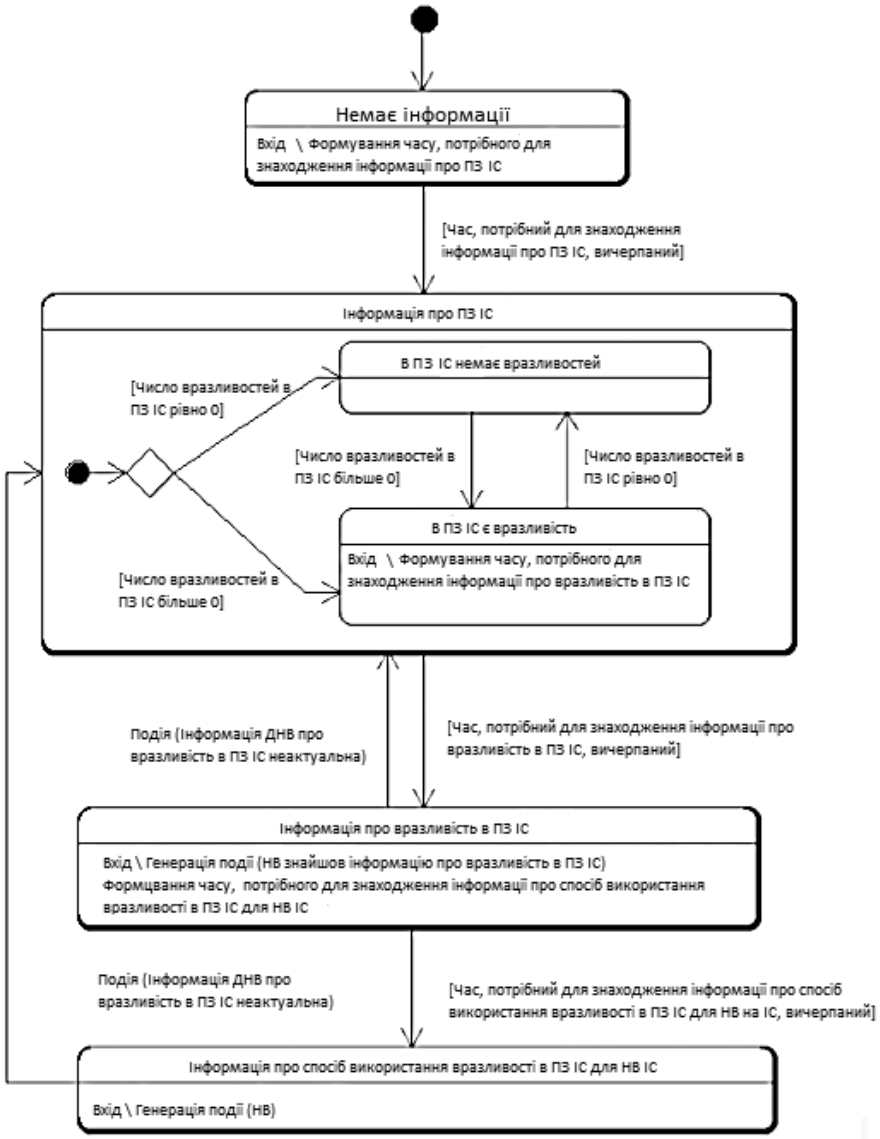


Рисунок 3.7 – Діаграма станів джерело негативного впливу в ході конфліктної взаємодії із інформаційною системою з відсутніми засобами захисту інформації

Відповідно до рисунку 3.7, джерело негативного впливу може бути в чотирьох станах:

– Стан «Про інформаційну систему відсутня інформація» – початковий стан, під час якого у джерела негативного впливу відсутня взагалі будь-яка інформація про інформаційну систему;

– Стан «Інформація про програмне забезпечення інформаційної системи» – стан, при якому у джерела негативного впливу є інформація про програмне забезпечення інформаційної системи;

– Стан «Інформація про вразливість в програмному забезпеченні інформаційної системи» – стан, при якому у джерела негативного впливу є інформація про програмне забезпечення інформаційної системи і про одну вразливість в цьому програмному забезпеченні;

– Стан «Інформація про спосіб використання вразливості в програмному забезпеченні інформаційної системи для негативного впливу на інформаційну систему» – стан, при якому у джерела негативного впливу є інформація про програмне забезпечення інформаційної системи, про одну вразливість в цьому програмному забезпеченні, а також дані як використати ці вразливості для здійснення негативного впливу на інформаційну систему.

Прогнозується, що джерело негативного впливу спочатку в стані «Про інформаційну систему відсутня інформація де формується час, необхідний негативному впливу для знаходження даних про програмне забезпечення інформаційної системи. Перехід до стану «Інформація про програмне забезпечення інформаційної системи» відбувається після виконання умови закінчення цього часу. Стан «Інформація про програмне забезпечення інформаійної системи» містить 2 підстани, «В програмне забезпечення інформаційної системи немає вразливостей» і «В програмному забезпеченні інформаційної системи є вразливості», в однин джерело негативного впливу потрапляє в залежності від кількості вразливостей в інформаційній системі. Якщо воно > 0 – то в стан «У програмному забезпеченні інформаційної системи є дефекти», якщо = 0 – то в стан «У програмному забезпеченні інформаційної системи відсутні дефекти». З цього випливає, що відбуваються зміни між цими підстанами. У підстанів «В програмне забезпечення інформаційної системи є вразливості» генерується час, який потрібний для пошуку однієї вразливості в програмне забезпеченні інформаційної системи Зміна стану на «Інформація про вразливість в програмне забезпеченні інформаційної системи» відбувається програмне забезпечення завершенню даного часу. Під час зміни даного стану генерується подія «джерело негативного впливу знайшов інформацію про вразливість в програмному забезпеченні інформаційної системи» і генерується час, який

необхідний для пошуку даних про спосіб використання вразливості в програмному забезпеченні інформаційної системи для негативнго впливу на інформаційну систему. Зміна стану «Інформація про спосіб використання вразливості в програмному забезпеченні інформаційної системи для негативного впливу на інформаційну систему» відбувається лише за умови завершення цього часу. При потраплянні до даного стан формується подія «Негативний вплив», через яку інформаційна система переходить до«Ненадійного стану». Є зміни станів «Інформація про вразливість» і «Інформація про спосіб використання вразливості для негативного впливу на інформаційну систему» на стан« Інформація про програмне забезпечення інформаційної системи в разі виникнення події« Інформація джерело негативного впливу про вразливість в програмному забезпеченні інформаційної системи неактуальна».

Отже, сукупність трьох діаграм станів, що на рисунках 3.1-3.3, відображає конфлікт між інформаційною системою з відсутніми засобами захисту інформації та джерелами негативного впливу, які намагаються здійснити негативний вплив на інформаційну систему та дозволяє розробити математичні моделі конфліктної взаємодії інформаційної системи з відсутніми засобами захисту інформації та джерела негативного впливу, та імітаційну модель конфліктної взаємодії з відсутніми засобами захисту інформації та джерела негативного впливу, за допомогою яких можна буде розрахувати ймовірність надійності інформаційної системи на протязі певного часу, інакше кажучи ймовірність непотрапляння інформаційної системи в «ненадійний стан» на протязі певного часу, і йімовірність знаходження інформаційної системи в «Надійному стані» протягом певного часового проміжку.

3.7 Об’єктно-орієнтована модель функціонування інформаційної системи з засобами захисту інформації в умовах конфліктних взаємодії із одним джерелом негативного впливу

Для конструювання об'єктно-орієнтованої моделі конфлікту так само, як і у випадку з інформаційною системою з відсутніми засобами захисту інформації, пропонується використовувати апарат мови UML [35]. Нижче на рисунках 3.8-3.11 наведені діаграми станів, які описують поведінку інформаційної системи, системного адміністратора і джерела негативного впливу.

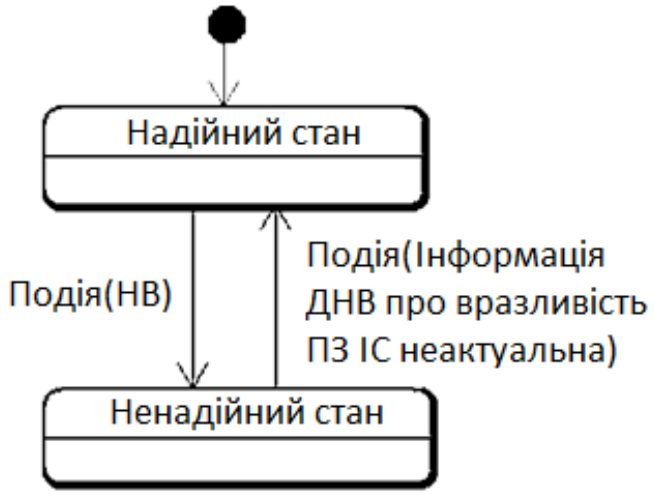


Рисунок 3.8 – Діаграма станів інформаційної системи з засобами захисту інформації в ході конфліктної взаємодії із джерелом негативного впливу

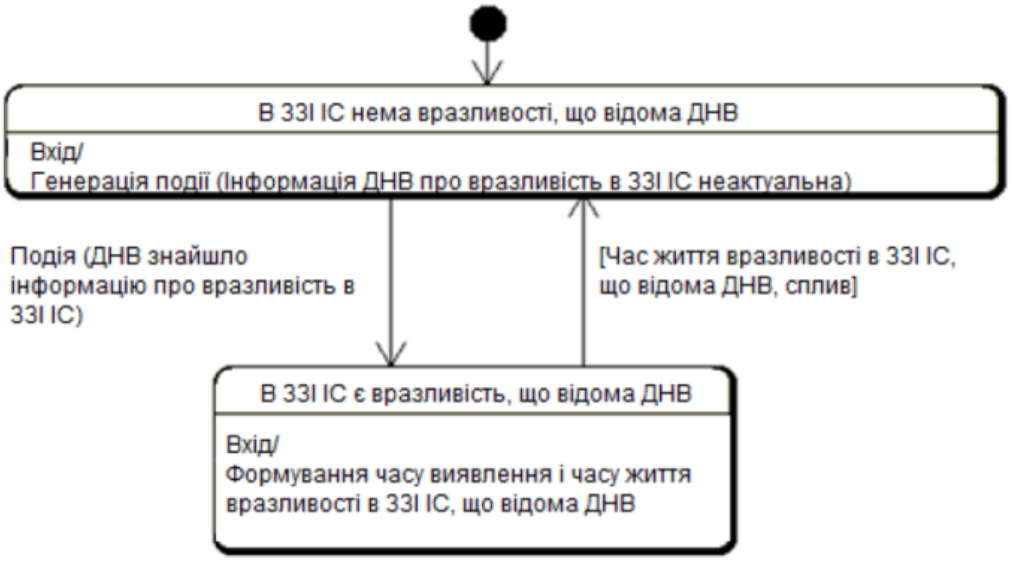


Рисунок 3.9 – Діаграма станів, що описує роботу системного адміністратора щодо закриття вразливостей в засобах захисту інформації, у ході конфлікту

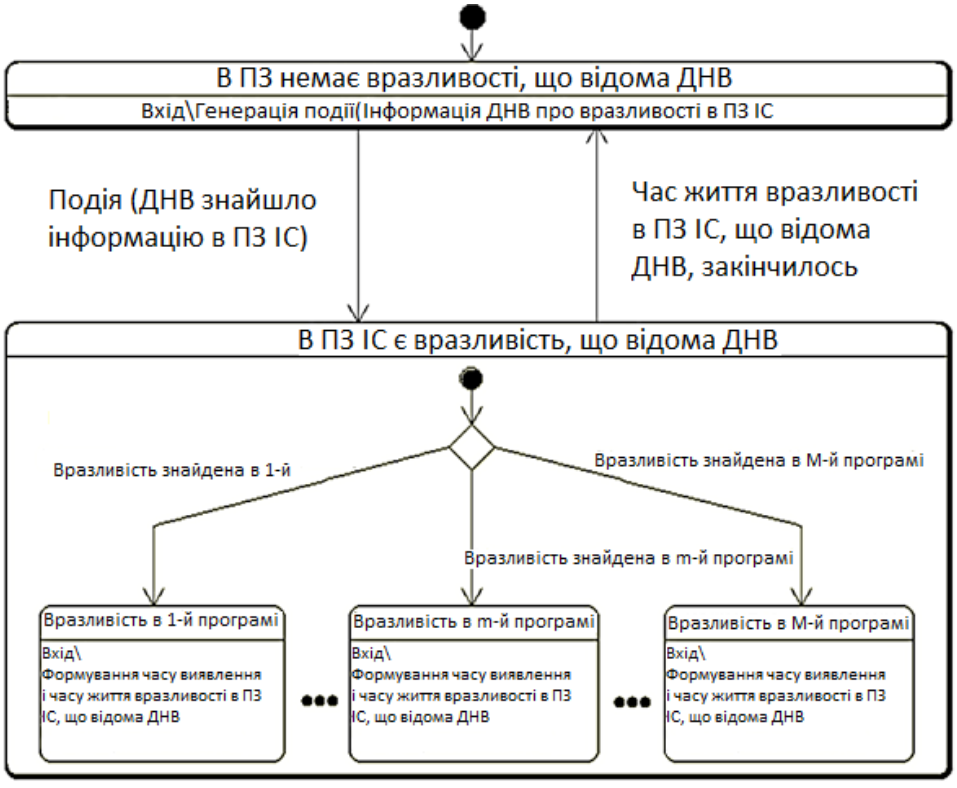


Рисунок 3.10 – Діаграма станів системного адміністратора в ході конфлікту системи з засобами захисту інформації з джерелом негативного впливу

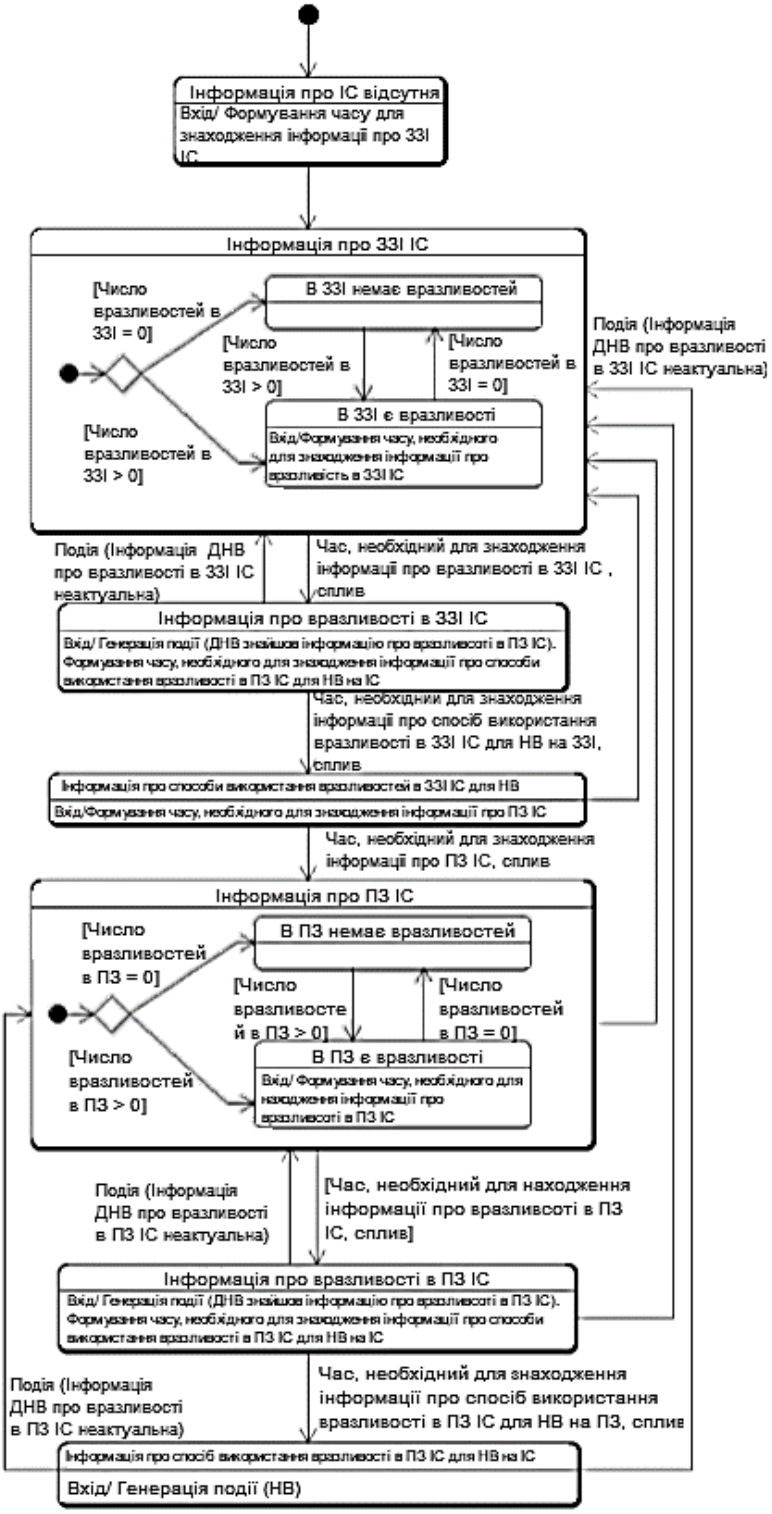


Рисунок 3.11 – Діаграма станів джерела негативного впливу в ході конфліктної взаємодії із інформаційною системою з засобом захисту інформації

Зміни об'єктно-орієнтованої моделі конфлікту інформаційної системи і одного джерела негативного впливу в порівнянні з випадком, коли інформаційна система не має засобів захисту інформації, виглядають наступним чином:

– тепер інформаційна система повертається зі стану «Ненадійний стан» в стан «Надійний стан» не лише при виникненні події «Інформація джерела негативного впливу про вразливість в програмному забезпеченні неактуальна», а й при виникненні події «Інформація джерела негативного впливу про вразливість в засобах захисту інформації неактуальна»;

– для моделювання процесу закриття вразливостей в засобах захисту інформації додана додаткова діаграма станів (Діаграма станів, що описує роботу системного адміністратора щодо закриття вразливостей в засобах захисту інформації, в ході конфліктної взаємодії системи з засобами захисту з джерелом негативного впливу, що на рисунку 3.9), аналогічна діаграмі станів, яка описує роботу системного адміністратора щодо закриття вразливостей в програмному забезпеченні, що на рисунку 3.10, з урахуванням того, що за припущенням в інформаційній системі є тільки один вид засобу захисту;

– у діаграму станів джерела негативного впливу, що на рисунку 3.8, додано 3 стани, що відображають його роботу з розвідки інформації для негативного впливу ще й на засіб захисту інформації («Інформація про засіб захисту інформаційної системи», «Інформація про вразливість у засобу захисту інформаційної системи», «Інформація про способи використання вразливості для негативного впливу на засіб захисту інформаційної системи»), подібні з аналогічними станами, що відображають процес розвідки інформації для негативного впливу безпосередньо на інформаційну систему (за винятком того, що в стані «Інформація про способи використання вразливості для негативного впливу на засіб захисту інформаційної системи» не генерується подія «Негативний вплив», а формується час, необхідний для знаходження інформації про програмне забезпечення), що їм передували;

– у діаграму станів джерела негативного впливу, що на рисунку 3.8, додані переходи в стан «Інформація про вразливість в засобі захисту інформації» з усіх

наступних станів за подією «Інформація джерела негативного впливу про вразливість в засобі захисту інформації неактуальна».

3.8 Об’єктно-орієнтована модель функціонування інформаційної системи в умовах конфліктних взаємодії із коаліцією джерел негативного впливу без інсайдера

Об'єктно-орієнтована модель конфлікту інформаційних систем без засобу захисту інформації і коаліції джерела негативного впливу без інсайдера будується аналогічно об'єктно-орієнтованої моделі конфлікту інформаційної системи з відсутніми засобами захисту інформації і одного джерела негативного впливу. При цьому в діаграму станів джерела негативного впливу додаються переходи, як на рисунку 3.12, пов'язані з отриманням інформації від інших джерел негативного впливу, що входять в коаліцію, тобто додаються такі переходи:

– Зі стану «Немає інформації» в стан «Є інформація про програмне забезпечення» при події «Джерело негативного впливу знайшло інформацію про програмне забезпечення інформаційної системи»

– Зі стану «Є інформація про програмне забезпечення інформаційної системи» в стан «Є інформація про вразливість в програмному забезпеченні інформаційної системи» при події «Джерело негативного впливу знайшло інформацію про вразливості в програмному забезпеченні інформаційної системи»

– Зі стану «Є інформація про вразливість в програмному забезпеченні інформаційної системи» в стан «Є інформація про спосіб використання вразливості в програмному забезпеченні інформаційної системи для негативного впливу на інформаційну систему» при події «Негативний вплив».

Подія «Джерело негативного впливу знайшло інформацію про програмне забезпечення інформаційної системи» генерується при вході будь-якого джерела негативного впливу в стан «Є інформація про програмне забезпечення інформаційної

системи». У загальну об'єктно-орієнтовану модель конфлікту включається стільки ж діаграм станів джерела негативного впливу скільки джерел негативного впливу входять в коаліцію і негативно впливають на інформаційну систему.

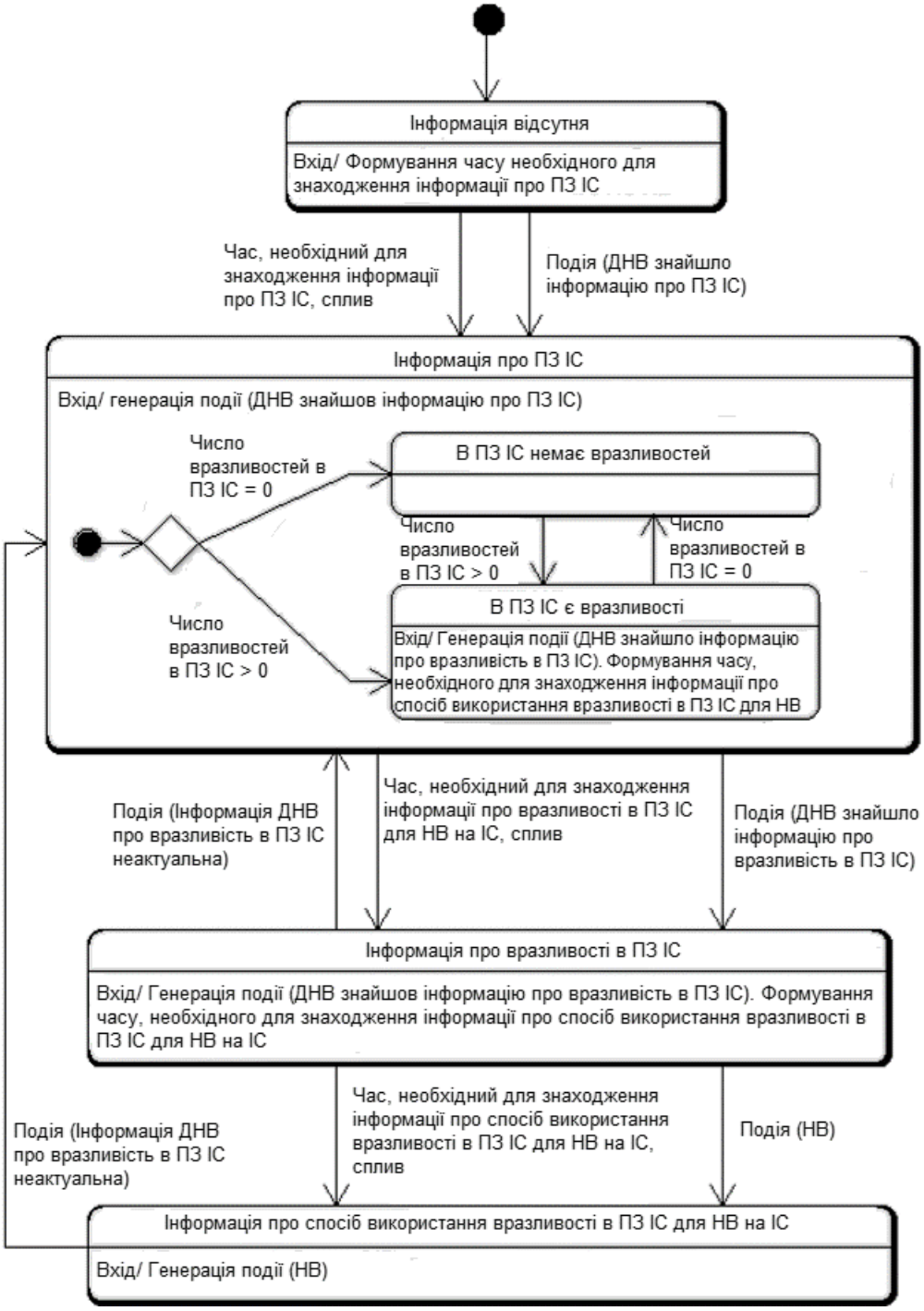


Рисунок 3.12 – Діаграма станів джерела негативного впливу в ході конфліктної взаємодії інформаційної системи з коаліцією джерел

3.9 Об’єктно-орієнтована модель функціонування інформаційної системи в умовах конфліктних взаємодії із коаліцією джерел негативного впливу з інсайдером

Об'єктно-орієнтована модель конфлікту інформаційної системи з відсутніми засобами захисту інформації і коаліції джерела негативного впливу з інсайдером аналогічна моделі конфлікту інформаційної системи з відсутніми засобами захисту інформації і коаліції джерела негативого впливу без інсайдера. Відмінністю є те, що в даному випадку додається, власне діаграма станів інсайдера, що на рисунку 3.13, яка відрізняється від діаграм станів джерел негативного впливу тим, що в ній відсутній стан «Інформація про спосіб використання вразливості в програмному забезпеченні інформаційної системи для негативного впливу на інформаційну систему».

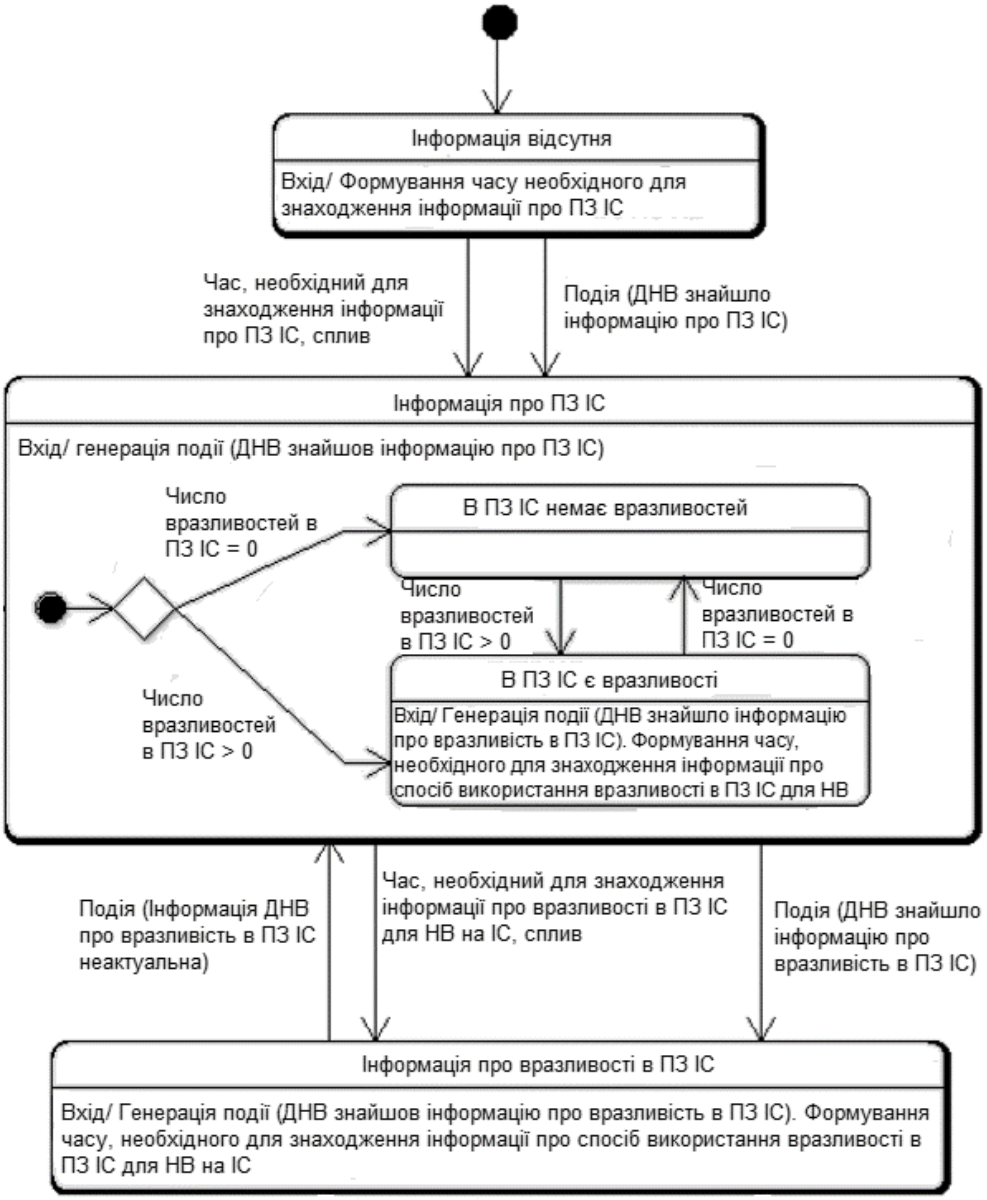


Рисунок 3.13 – Діаграма станів інсайдера у ході конфліктної взаємодії інформаційної системи з інсайдером

4 РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

4.1 Розробка імітаційної моделі конфліктної взаємодії інформаційної системи з джерелом негативного впливу

Представлена математична модель конфліктної взаємодії інформаційної системи з джерелом негативного впливу може враховувати лише середнє значення середньостатистичної кількості вразливостей, які перебувають в програмному забезпеченні інформкаційної системи, за проміжок конфлікту, тоді як в реальнму житті середньостатистична кількість вразливостей у програмному забезпеченнні інформаційної системи протягом заданого періоду може змінюватися. Окрім цього, реальний розподілений час переходів до різних станів може мати довільний характер, відмінний від пуассонівської моделі. До того ж часто трапляється необхідність розглядання ситуації, яка може принципово відрізнятися від дуелної, особливо у випадку конфлікт стосується кількох учасників з кожної сторони, наприклад, на інформаційну систему здійснюють атаку не один, а декілька джерел нагативного впливу.

Необхідність враховування усіх важливих для опису конфліктнї взаємодії факторів та ускладнення постановки задачі неминуче призводять до все більших ускладнень при застосуванні математичних аналитичних моделей, для дослідження закономірностей конфлікту визначається значна роль комп’ютерних засобів та технологій об’єктно-орієнтованого моделювання. Один з популярних комп’ютерних засобів і підходящим для того, щоб описувати динаміки ситуаційного конфлікту механізмом реалізації комп’ютерних імітаційних моделей інформаційного конфлікту систем є застосування формалізму гібридних автоматів, а саме карт станів Харела, а також можливостей, які представляє інтегроване середовище MATLAB + Simulink + Stateflow для реалізації даних задач [17, 30, 31, 32].

Представлення моделі у Simulink середовищі зображено на рисунку 3.1. У представленому випадку, для проведення різних експериментів, використане наступне можливе подання різних даних, таких як:

– t – визначення імітаційного часу, що дозволяє проводити дослідження імітаційного характеру за чітко визначений проміжок часу;

– nvrazlyv – середньостатичне число вразливостей в інформаційній системі – інформація, яка має особливість змінюватися з часом, тому необхідно мати можливість змінювати їх;

– nvrazlyv1 та nvrazlyv2 – середньостатичне число вразливостей в програмному забезпеченні. 1 та 2 – інформація, яка буде різною при імітаційному моделюванні різних програмних забезпечень, тому необхідно мати можливісь задавати їх мануально, вводити;

– T_{po} – середній час джерела негативного впливу для того, щоб знаходити дані про програмне забезпечення;

– T_{uazv} – середній час джерела негативного впливу для того, щоб знаходити дані про всі вразливості в інформаційній системі;

– T_{nv} – середній час джерела негативного впливу для того, щоб знаходити дані про спосіб використання вразливості в програмному забезпеченні інформаційної системи;

– K – кваліфікація адміністратора, його коефіцієнт.

– T_{v1}, T_{v2}, T_{v3} – час, за який вендору необхідно випустити патчі для закрится вразливостей в програмному забезпеченні 1, програмному забезпеченні 2, програмному забезпеченні 3.

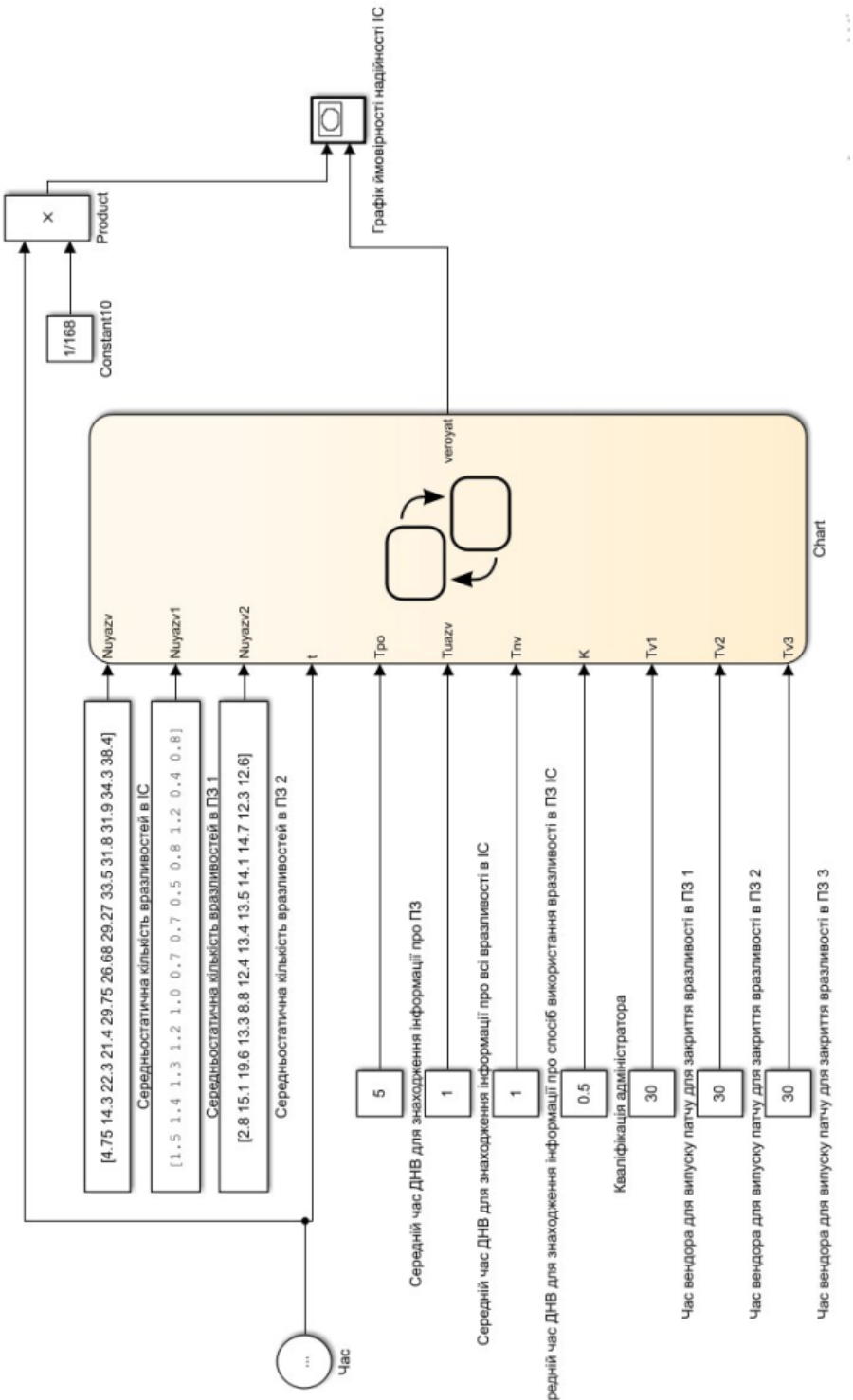


Рисунок 4.1 – Simulink-модель конфліктної взаємодії

Конфліктну взаємодію інформаційна система – джерело негативного впливу в термінах [36] можна представити за допомогою SF-моделі зображеній на рисунку 4.1.

Дана модель ґрунтується на представленій раніше сукупності діаграм станів інформаційної системи, системного адміністратора і джерела негативного впливу, наведених вище на рисунках 3.5-3.7. Модель складається з трьох паралельно функціонуючих об'єктів «Sysadmin» та «IS» з однієї сторони та «DNV» з іншої сторони, власне всередині яких знаходяться карти станів, які описують потенційні значення враховуваних чинників та поведінку всіх сторін, які беруть участь у конфлікті, залежно від даних значень.

Інформаційна система, яку представляє блок «IS» може перебувати у головних двух станах:

– Стан «Nadiyny_stan» – стан, при якому інформаційна система вважається захищеною від негативного впливу джерела негативного впливу, відповідає стану «Надійний стан» в об'єктно-орієнтованій моделі.

– Стан «Nenadiyny_stan» – стан, при якому інформаційна система вважається незахищеною від негативного впливу джерела негативного впливу, відповідає стану «Ненадійний стан» в об'єктно-орієнтованій моделі.

За допомогою блоку «Sysadmin» імітується робота системного адміністратора стосовно усунення дефектів, що відомі джерелу негативного впливу, і передбачається можливість знаходження в двух станах:

– Стан “Nema_izv_DNV_vrazlyv» – стан, при якому адміністратор інформаційної системи готується закривати вразливості в програмному забезпеченні, відповідає стану «В програмному забезпеченні інформаційної системи немає вразливості, відомої джерелу негативного впливу» в об'єктно-орієнтованій моделі.

– Стан «Ye_vidoma_DNV_vrazlyv» – стан, при якому адміністратор інформаційної системи закриває вразливість у програмному забезпеченні, яка відома джерелу негативного впливу, відповідає стану «У програмному забезпеченні інформаційної системи є відома джерелу негативного впливу вразливість» в об’єктно-орієнтованій моделі.

Для визначеності будемо вважати, що в інформаційній системі встановлено три види програмного забезпечення. Тоді стан «Ye_vidoma_DNV_vrazlyv» необхідно розділити на три підстани:

– «Vrazlyv_v_1_programmi»,
– «Vrazlyv_v_2_programmi»,
– «Vrazlyv_v_3_programmi».

Вірогідність потрапити в один із даних станів можна визначити за наступною логікою: при потраплянні до стану «Ye_vidoma_DNV_vrazlyv» змінній Ppo присвоюється величина, що є випадковою та розподіленою на відрізку від 0 до 1 рівномірно. Даний відрізок ділиться на три інтервали, кожному з яких у відповідність ставиться вид програмного забезпечення, де був знайдений дефект. Довжина кожного інтервалу рівняється відношенню середньостатистичної кількості вразливостей у програмному забезпеченні, якому у відповідність поставлений даний інтервал, до середньостатистичної кількості вразливостей у інформаційній системі, тобто конкретно з трьома навними програмними додатками [0,1] будет розбитий на інтервали [0, Nvrazlyv1/Nvrazlyv], [(Nvrazlyv1/Nvrazlyv, (Nvrazlyv1+Nvrazlyv2)/Nvrazlyv] та , [(Nvrazlyv1+Nvrazlyv2)/Nvrazlyv),1]. У випадку значення змінної Ppo потрапить до 1-го інтервалу, то блок «Sysadmin» потрапить до підстану «Vrazlyv_v_1_programmi», якщо до в 2-го – то в «Vrazlyv_v_2_programmi», а якщо до 3-го – то в «Vrazlyv_v_3_programmi». Таким самим чином доступне моделювання випадків, коли в інформаційній системі встановлена більша або менша кількість програм.

Упереджувальний перехід до стану «Nema_vidom_DNV_vrazlyv» викликає генерацію події “Nema_inf_vrazlyv», яка переводить блок «DNV» з будь-якого стану, крім «Nema_informacii», в стан «Informaciya_pro_PZ», що означає, що інформація про способи взлому та доступ до вразливостей, які на той момент відомі джерелу негативного впливу, втрачають актуальність. При цьому блок «IS» переходить в стан «Nadiyny_stan», що відповідає переходу інформаційної системи в надійний стан.

Стани сторони «DNV», в яких вона може знаходитись, є повністю відповідними станам джерела негативного впливу, визначеним у розглянутій вище об’єктно-орієнтованій моделі конфлікту інформаційної системи і джерела негативного впливу:

– Стан “Nema_informacii» – початковий стан, при якому у джерела негативного впливу відсутня будь-яка інформація про систему.

– Стан «Informaciya_pro_PZ» – стан, при якому у джерела негативного впливу є інформація про програмне забезпечення інформаційної системи.

– Стан «Informaciya_pro_vrazlyvosty» – стан, при якому у джерела негативного впливу є інформація про програмне забезпечення інформаційної системи і про одну вразливість в цьому програмному забезпеченні.

– Стан «DNV_informaciya_pro_sposoby_nv» – стан, при якому у джерела негатвного впливу є інформація про програмне забезпечення інформаційної системи, хоча б про одну вразливість в цьому програмному забезпеченні, а також вразливості для здійснення негативного впливу на інформаційну систему.

Стан «Informaciya_pro_PZ» містить в собі 2 підстани:

– “Nema_vrazlyv»,

– «Est_vrazlyv».

– У підстан “Nema_vrazlyv» блок «DNV» потрапляє у випадку, якщо середньостатистична кількість вразливостей в інформаційній системі дорівнює 0, в підстан «Est_vrazlyv», якщо – більше 0. Упереджувальний перехід в стан «Informaciya_pro_vrazlyvimosty» забезпечує генерацію події «inf_vrazlyv», яка переводить блок «Sysadmin» в стан «Ye_vidoma_DNV_vrazlyv». При упереджувальному досягненні останнього стану генерується власне подія «nv», що переводить блок «IS» в стан «Nenadiyny_stan», який відповідає переходу інформаційної системи в ненадійний стан.

Час переходу сторони «DNV» у будь-який з можливих станів описується змінною t_1. Час знаходження джерела негативного впливу, тобто сторони «DNV», у станах “Nema_informaci» та «Informaciya_pro_vrazlyvimosty» за умови відсутньої

події “Nema_inf_vrazlyv» at_1 є величиною випадковою і формується наступним чином: ml('(1/(1/%f))*log(rand)*(-1)', Tpo). Завдяки цьому визначається випадкове число, розподілене за експоненціальним законом з параметром джерела негативного впливу, що складає $1/T_{ПЗ}$, $1/T_{НВ}$ в залежності від стану. Час перебування джерела негативного впливу в стані «Informaciya_pro_PZ» at_{11} становить ml('(1/(1/%f))*log(rand)*(-1)', Tuazv), що означає відношення загального часу, потрібного джерелу негативного впливу для знаходження інформації про всі слабкі місця в програмному забезпеченні інформаційної системи, до числа цих вразливостей. Переходи з одного стану в інший відбуваються за умови закінчення часу знаходження в кожному з станів.

Тривалість життя вразливості, що відома джерелу негативного впливу для першої програми розраховується наступним чином $at_2 = ml('(1/(\%f/\%f))*log(rand)*(-1)', K, Tv1)$, відповідно для другої програми , $at_2 = ml('(1/(\%f/\%f))*log(rand)*(-1)', K, Tv2)$ та відповідно для третьої програми $at_3 = ml('(1/(\%f/\%f))*log(rand)*(-1)', K, Tv3)$. Час виявлення дефекту, що відомий джерелу негативного впливу, $t_2 = t\text{-}rand \cdot at_2$, де t – поточний час, що означає, що час виявлення дефектує величиною випадковою, яка з однаковою йімовірністю приймає параметри з інтервалу від різниці поточного часу та часу існування дефекту до поточного часу. Варто зазначити, що на вид законів розподілення в цілому обмежень не існує у даній моделі.

На відміну від моделей конфліктної взаємодії, що розглянуті у [17], жодна зі сторін у запропонованій моделі не може бути абсолютним переможцем. Це значить, що у випадку переходу інформаційної системи до «Ненадійного стану», є можливість повернутися знову до надійного.

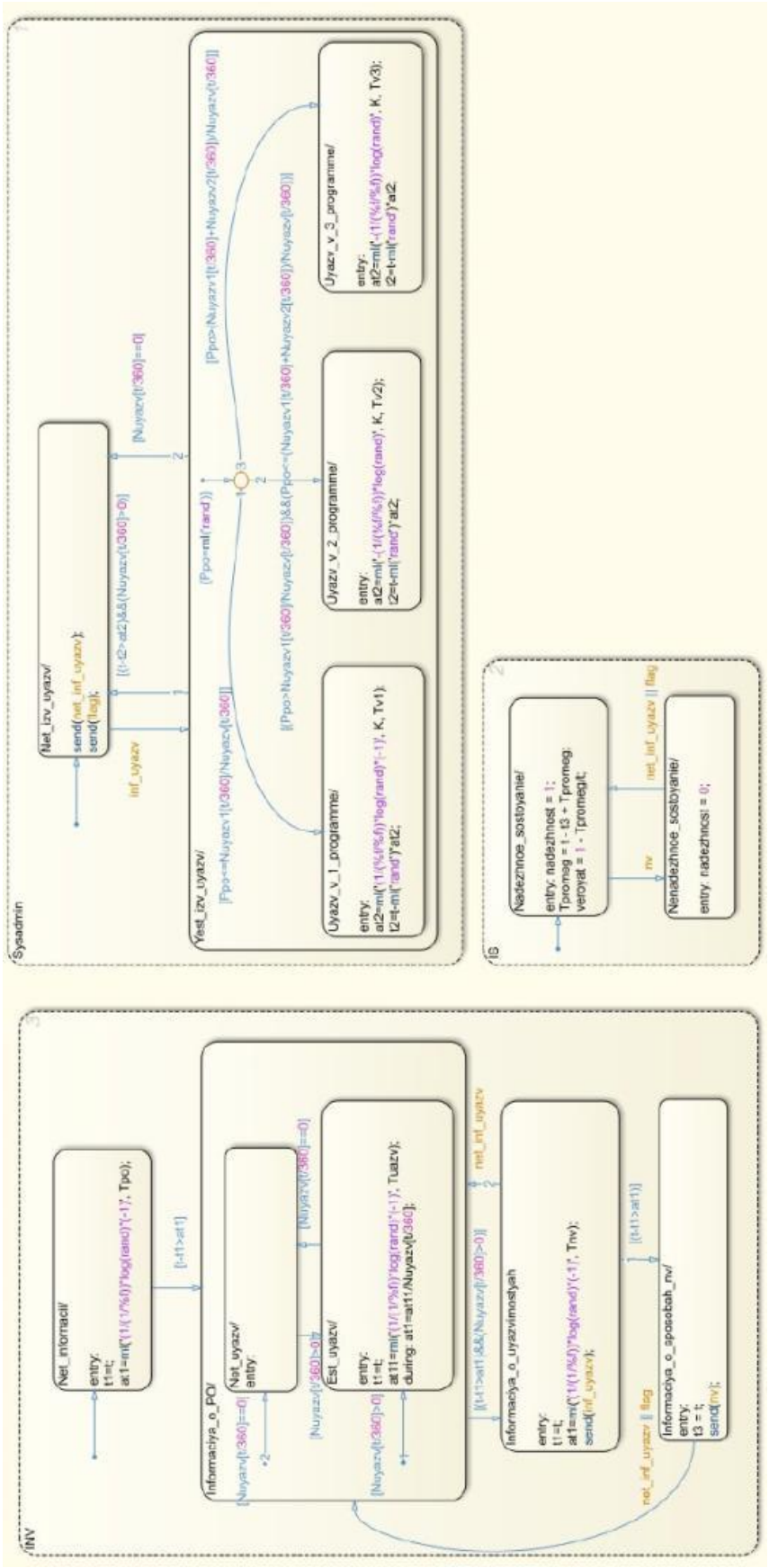


Рисунок 4.2 – SF-модель конфлікту інформаційної системи і одного джерела негативного впливу

4.2 Розробка імітаційної моделі інформаційної системи в умовах конфліктних взаємодії із наявним засобом захисту інформації в інформаційній системі

Для того, щоб імітаційна модель конфлікту інформаційної системи та одного джерела негативного впливу враховувала наявність засобу захисту інформації в ній, необхідно виконати дії, схожі на дії в об'єктно-орієнтованій моделі. Додається ще одна подія, яка переводить блок «IS» в стан «Nenadiyny_stan» - "Nema_inf_vrazlyv_ZZI», що відображає втрату актуальності інформації, якою володіє джерело негативного впливу про вразливість в засобі захисту інформації. Блок «Sysadmin» розділяється на 2 підблоки, один з яких як і раніше, моделює процес закриття вразливостей в програмному забезпеченні, а інший, з урахуванням того, що в системі встановлений один вид засобу захисту інформації моделює процес закриття вразливостей в засобі захисту інформації, що відомі джерелу негативного впливу.

У блок «DNV» додаються стани, що визначають поведінку розвідки інформації про засіб захисту інформації для негативного впливу на нього. Це блоки «Informaciya_pro_ZZI»,«Informaciya_pro_vrazlyv_ZZI», «Informaciya_pro_sposoby_nv_ZZI», переходи блоку «DNV» в стани, що відповідають наявності інформації про засоби захисту інформації «Informaciya_pro_ZZI» із всіх наступних станів при виникненні події "Nema_inf_vrazlyv_ZZI».

Окремі блоки імітаційної моделі «DNV», «Sysadmin» та «IS» з внесеними змінами зображені на рисунках 4.3, 4.4 та 4.5 відповідно. Загальна модель конфлікту системи з засобом захисту інформації та одного джерела негативного впливу зображена на рисунку 4.6.

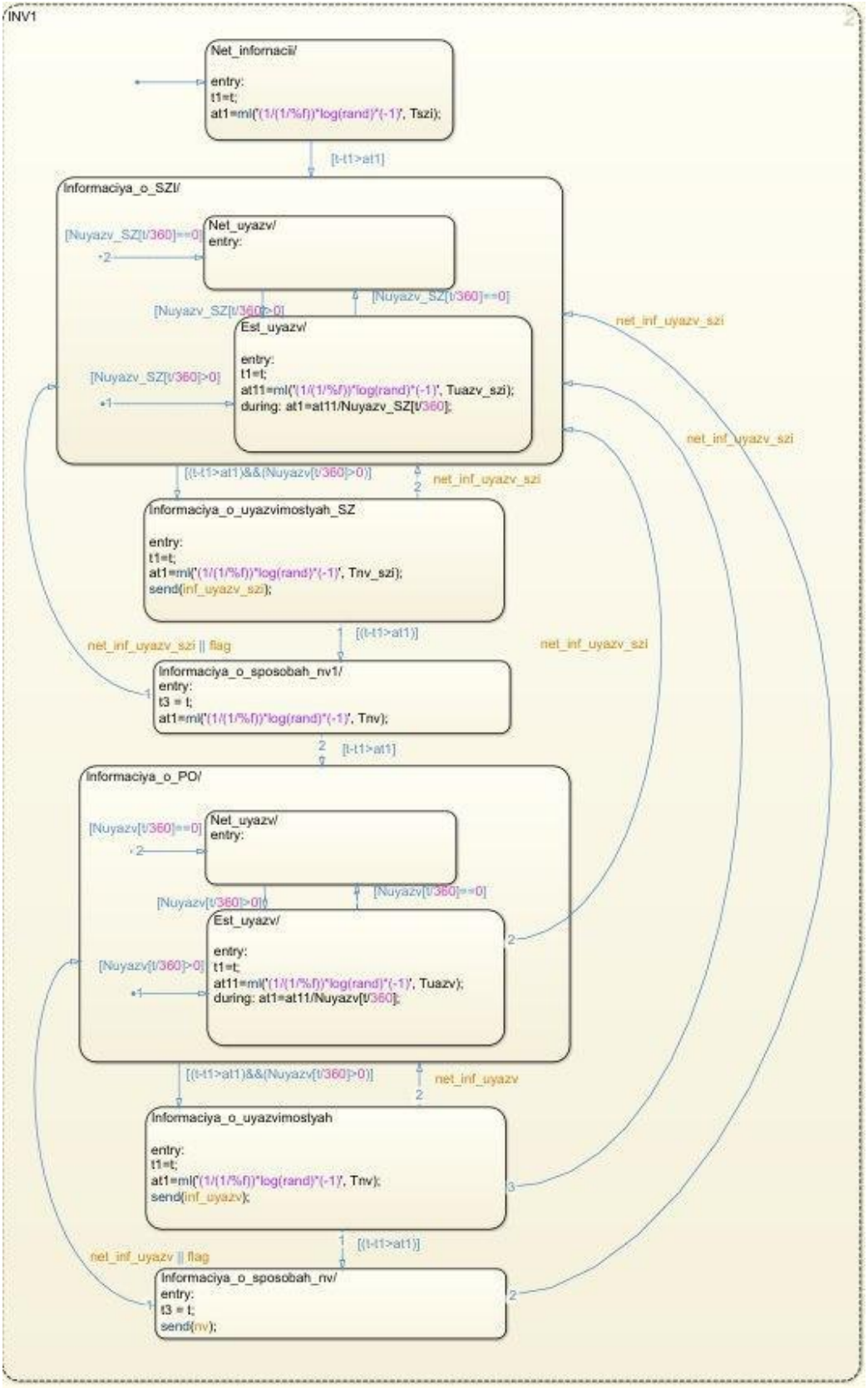


Рисунок 4.3 – Блок джерела негативного впливу

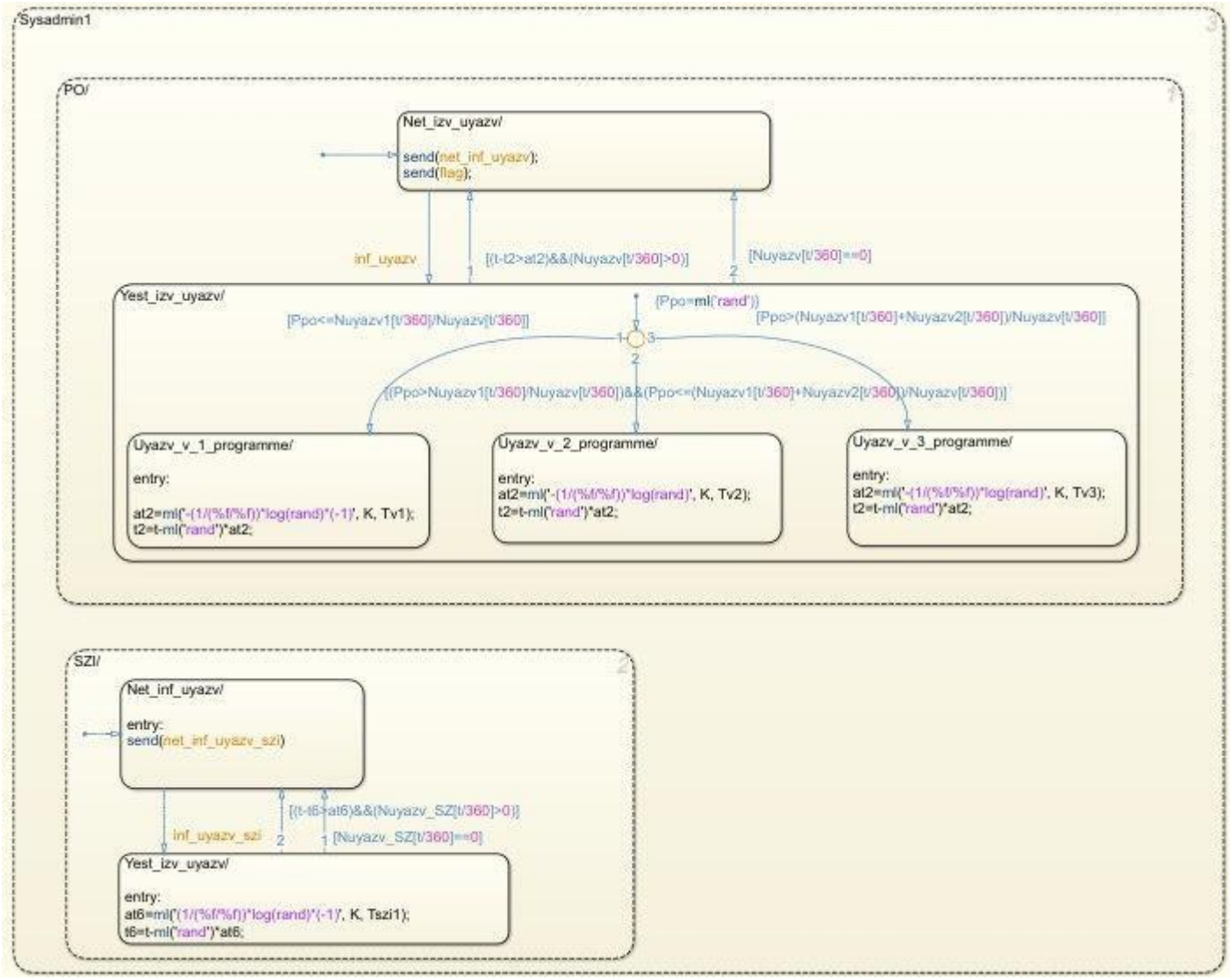


Рисунок 4.4 – Блок системного адміністратора

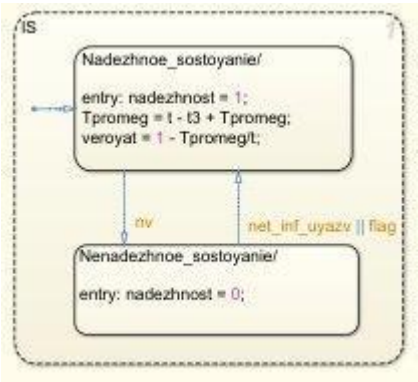


Рисунок 4.5 – Блок інформаційної системи

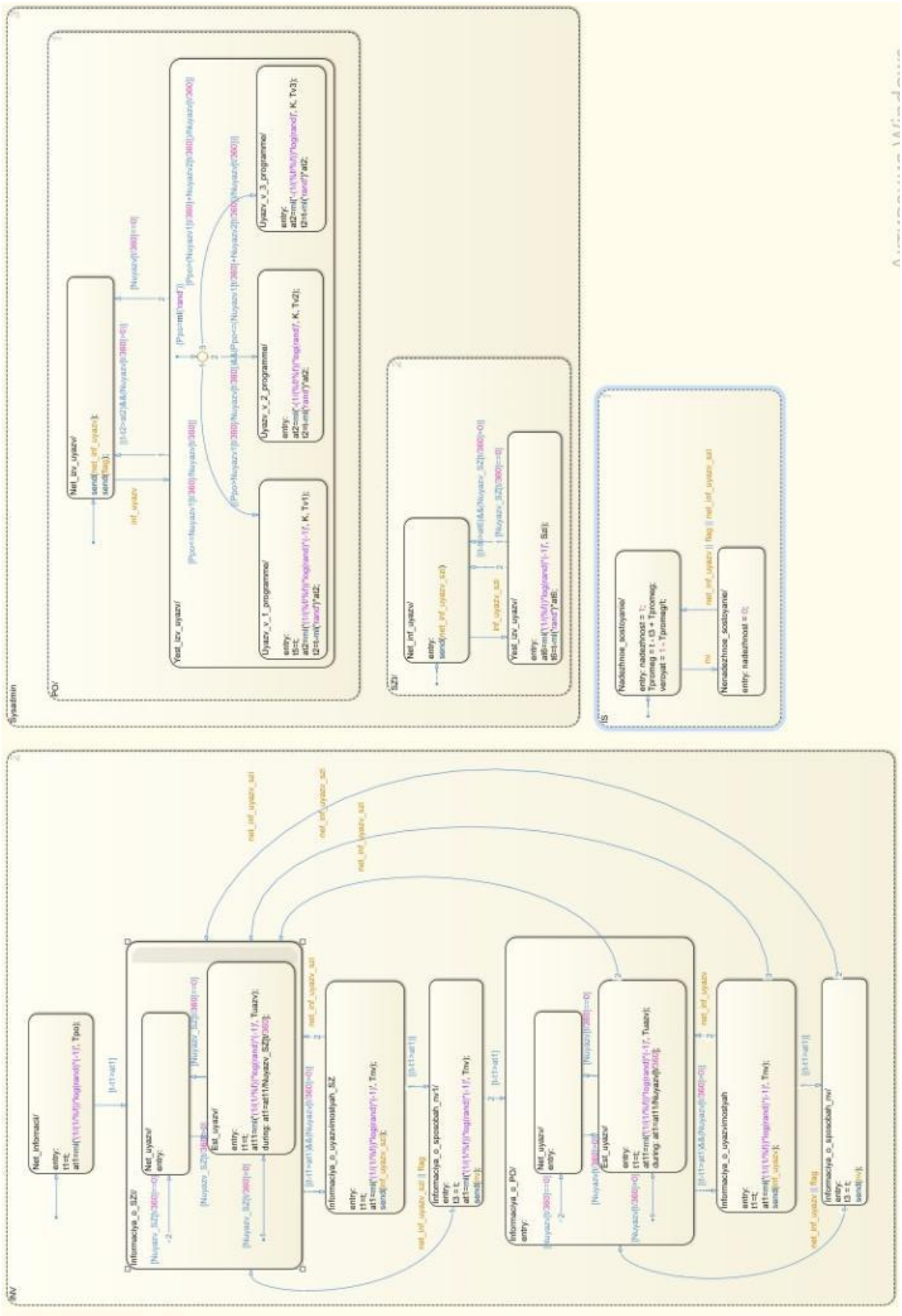


Рисунок 4.6 – Загальна імітаційна модель конфлікту з засобом захисту

4.3 Розробка імітаційної моделі інформаційної системи в умовах конфліктних взаємодії із коаліцією джерел негативного впливу без інсайдера

Зміни в імітаційній моделі конфлікту інформаційної системи і коаліції джерел негативного впливу аналогічні змінам в об’єктно-орієнтованій моделі. Додаються декілька додаткових блоків «DNV», в залежності від кількості джерел негативного впливу, кожен з яких відповідає конкретному джерелу, як на рисунку 4.7. У кожному блоці, що відповідає за дії конкретного джерела негативного впливу, додаються переходи, що пов’язані з обміном інформацією між джерелами (при виникненні події «inf_PZ»). У кожному блоці «DNV» при вході в стан «Informaciya_pro_PZ» генерується дана подія. У блоки «Sysadmin» та «IS» ніякі зміни не вносяться. Повна модель конфлікту інформаційної системи та коаліції джерел негативного впливу зображена на рисунку 4.8.

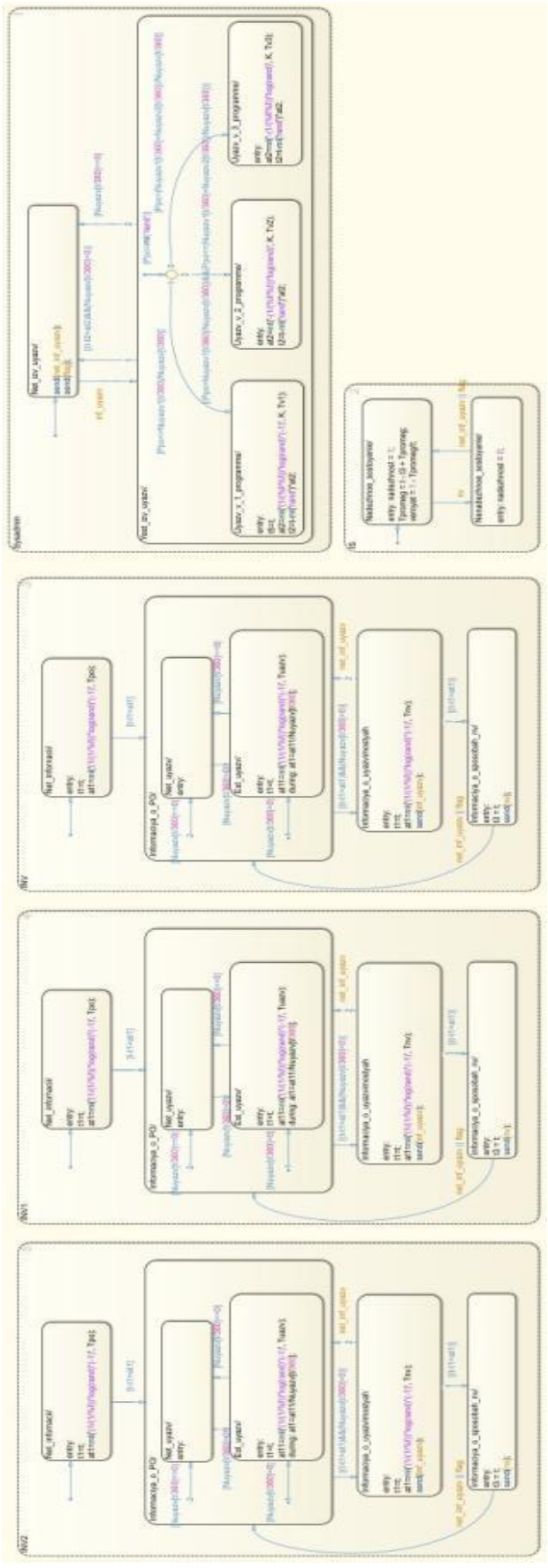


Рисунок 4.8 – Загальна імітаційна модель конфлікту з коаліцією джерел

4.4 Розробка імітаційної моделі інформаційної системи в умовах конфліктних взаємодії із коаліцією джерел негативного впливу з інсайдером

Зміни і імітаційній моделі конфлікту інформаційної системи і коаліції джерел негативного впливу з інсайдером аналогічні змінам в об'єктно-орієнтованій моделі. А саме додається блок «INS», що на рисунку 4.9, який є аналогічним блоку «DNV», але немає стану «Informaciya_pro_sposoby_nv».

Загальна схема представлена на рисунку 4.10

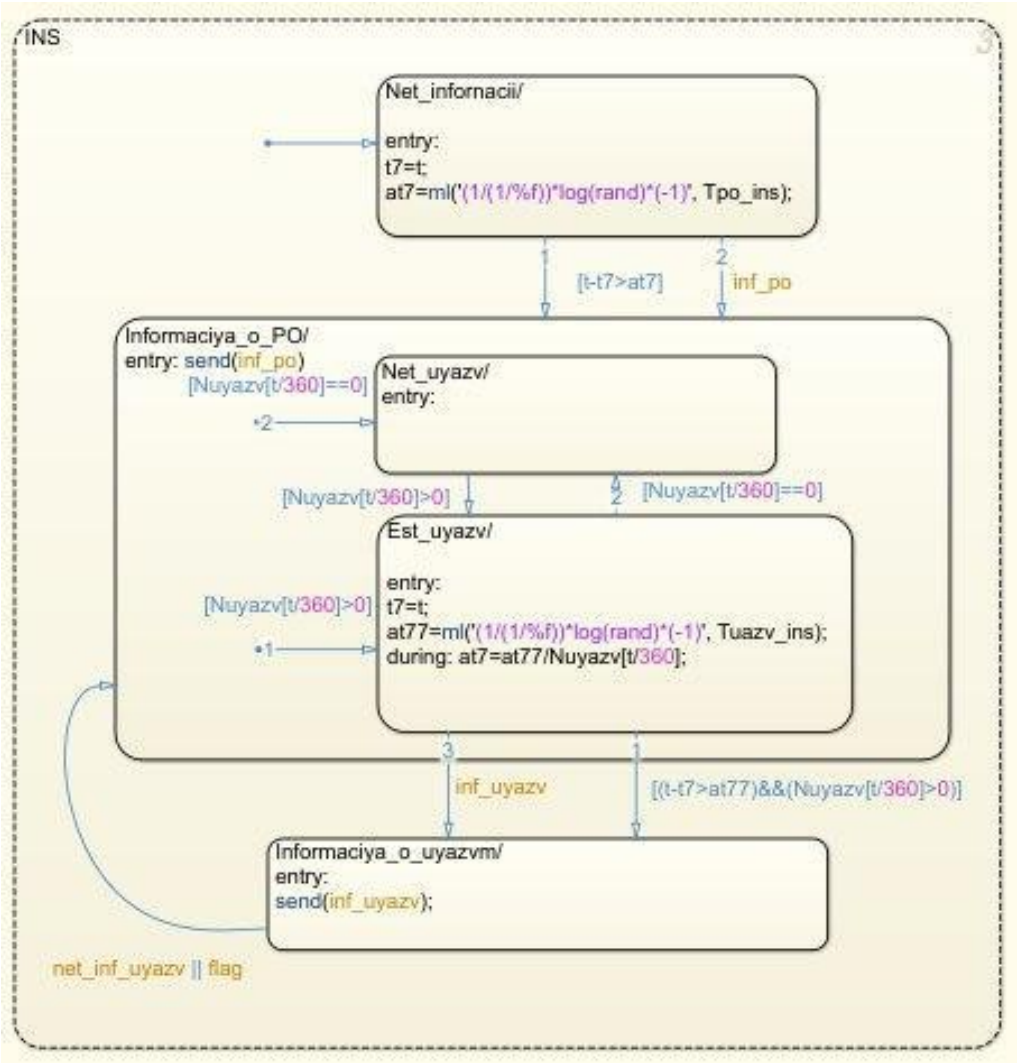


Рисунок 4.9 – Блок інсайдера

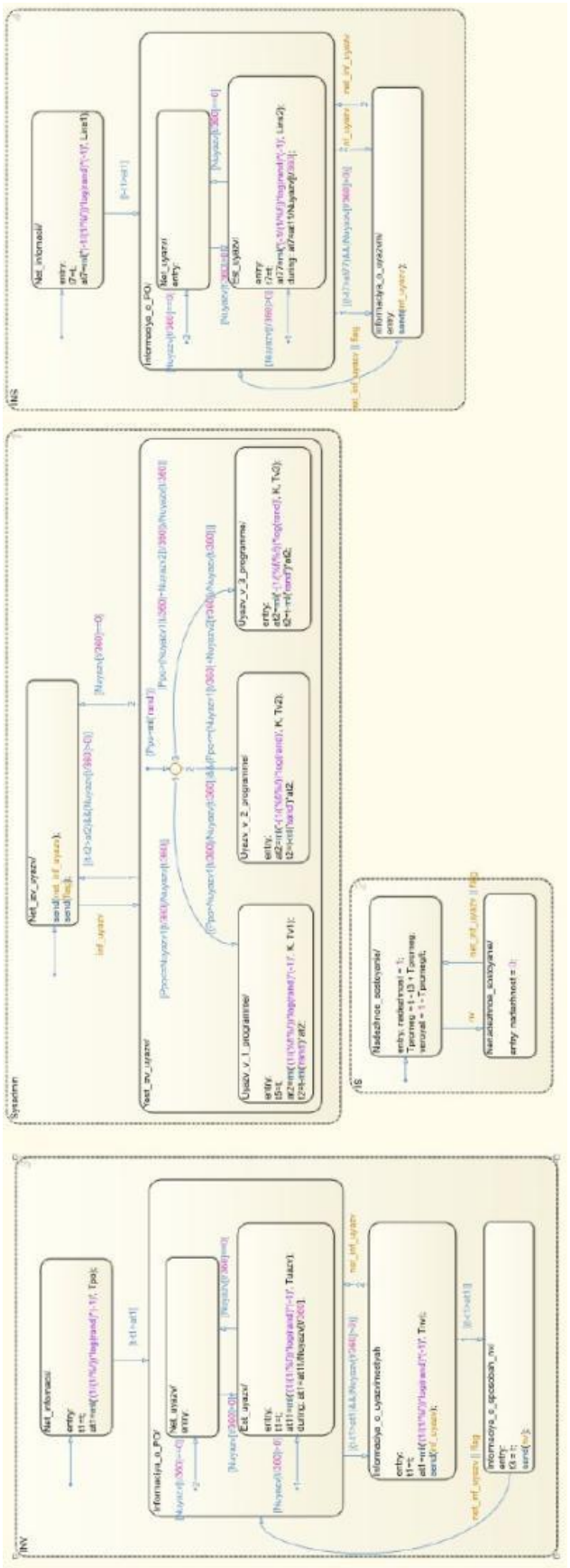


Рисунок 4.10 – Загальна імітаційна модель конфлікту з коаліцією джерел з інсайдером

4.5 Порівняння математичної та імітаційної моделей

– Для порівняння імітаційної та математичної моделі, розрахуємо ймовірність надійності інформаційної системи для Windows 10, при умові, що інформаційна система встановлена на операційній системі Windows 10. Потрібні статистичні дані відносно програмного забезпечення використані з [6-8]. Розрахунок пропонується здійснити для джерел негативного впливу 4 різних рівнів кваліфікації:

– 1-ї категорії ($T_{ПЗ}$ = 60 днів, $T_{вразл}$ = 30 днів,$T_{нв}$ = 30 днів);

– 2-ї категорії ($T_{ПЗ}$ = 20 днів, $T_{вразл}$ = 30 днів,$T_{нв}$ = 10 днів);

– 3-й категорії ($T_{ПЗ}$ = 10 днів, $T_{вразл}$ = 5 днів,$T_{нв}$ = 5 днів);

– 4-ї категорії ($T_{ПЗ}$ = 5 днів, $T_{вразл}$ =1 день,$T_{нв}$ = 1 день).

– Нижче на рисунках 4.11-4.12 наведені графіки ймовірності надійності системи з операційною системою Windows 10 без та з засобом захисту інформації під час спроби впливу на неї джерел негативного впливу 1-4 категорій.

Абсолютне максимальне середнє відхилення йімовірності надійності інформаційної системи, яке розраховане з використанням математичної моделі, від імовірності надійності інформаційної системи, яка розрахована з використанням імітаційної моделі, без засобу захисту інформації склало 7%,а з ним - 9%. Різниця результатів з використанням математичної і імітаційної моделей випливає з того, що мат модель не бере до уваги зміну кількості вразливостей в системі на протьязі конфлікту.

При використанні цих двух моделей може бути знайдена ймовірність дефекту надійності інформаційної системи вразливостями в конкретному програмному забезпеченні, а також час, необхідний джерелу негативного впливу щоб успішно вплинути на систему, а з використанням імітаційної моделі потенційну кількість успішних впливів на систему та середній час сталого перебування системи в ненадійному стані. Ці величини відповідно можуть описати надійність використання програмного забезпечення в інформаційній системі в умовах конфліктних взаємодій.

Позначки:

– синій – ймовірність надійності під час атаки джерела негативного впливу 1-ї категорії;

– жовтий – ймовірність надійності під час атаки джерела негативного впливу 2-ї категорії;

– бордовий – ймовірність надійності під час атаки джерела негативного впливу 3-ї категорії;

– зелений – ймовірність надійності під час атаки джерела негативного впливу 4-ї категорії;

Кружечками позначено математичні розрахунки надійності відповідних джерел.

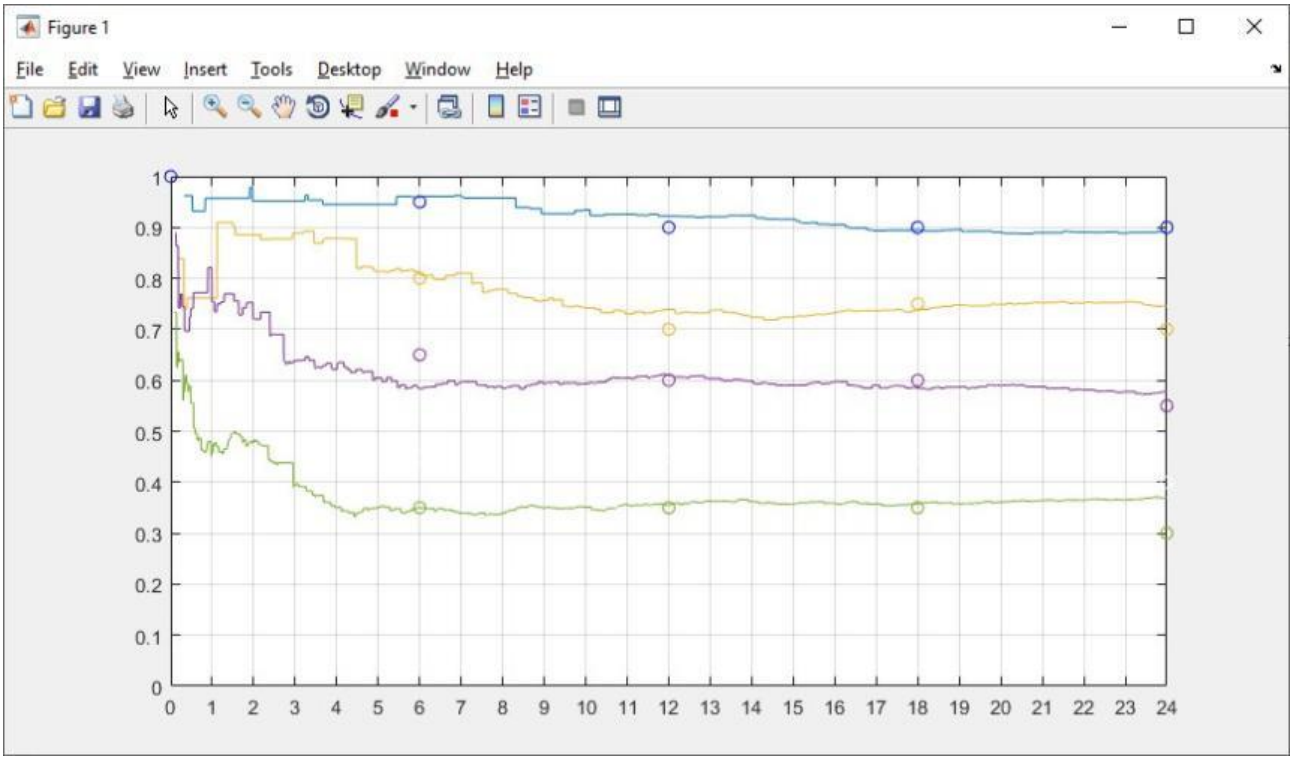


Рисунок 4.11 – Ймовірність надійності інформаційної системи з операційною системою Windows 10 при спробі негативного впливу на неї джерела негативного впливу 1ї, 2ї, 3ї, 4ї категорій і коефіцієнтах роботи системного адміністратора:k=3

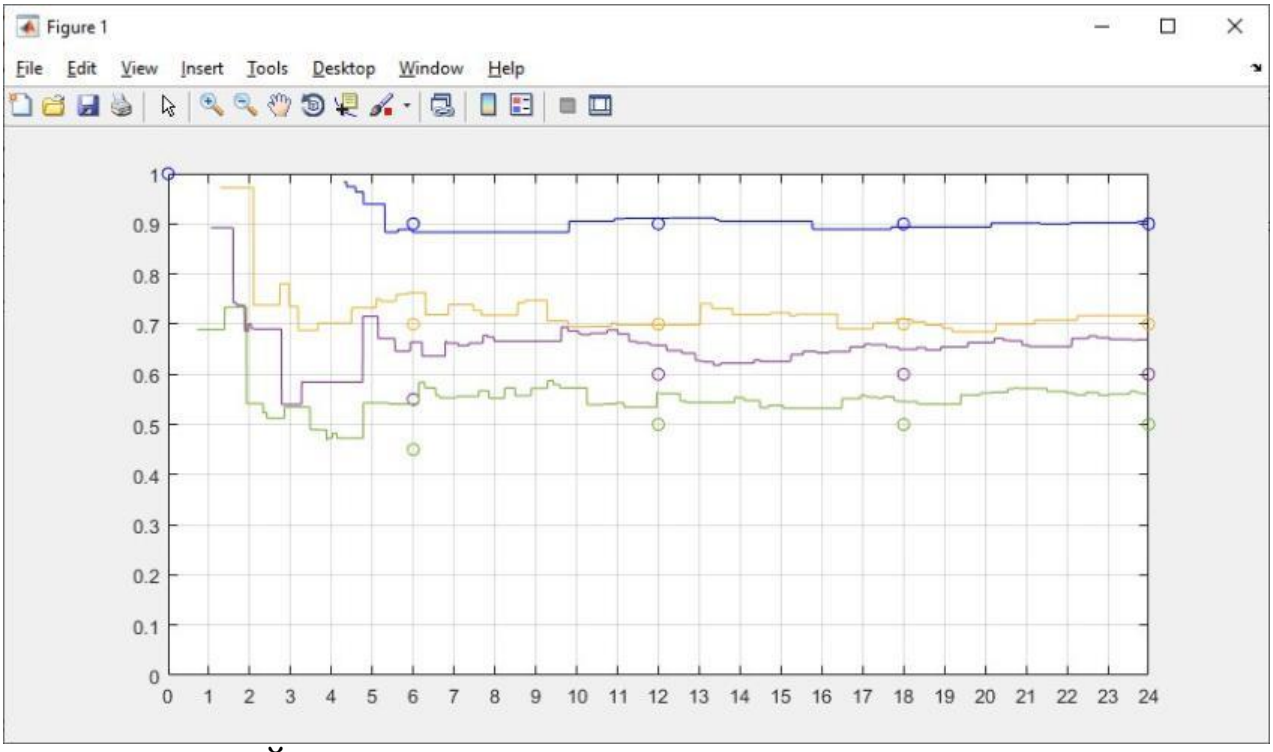


Рисунок 4.12 – Ймовірність надійності інформаційної системи з операційною системою Windows 10 із засобом захисту інформації при спробі негативного впливу на неї джерела негативного впливу 1ї, 2ї, 3ї, 4ї категорій і коефіцієнтах роботи системного адміністратора:k=0,5

4.6 Приклад моделювання конфліктної взаємодії в типовій інформаційній системі

Характеризуючи розроблені математичні та комп'ютерні моделі варто зазначити, що вони легко можуть бути вдосконалені на основі більш точного врахування поведінки джерел негативного впливу і системного адміністратора, складу інформаційної системи, а також параметрів, що впливають на поведінку, наприклад, врахування наявності експлойтів для вразливостей, наявність в інформаційній системі систем виявлення вторгнень або засобів обману джерел негативного впливу тощо. Для таких змін немає необхідності міняти всю концепцію, а досить додати нові стани і (або) переходи, а в імітаційну модель також, можливо – нові блоки і підблоки.

На рисунку 4.13 продемонстровано приклад моделювання типової можливої конфліктної взаємодії:

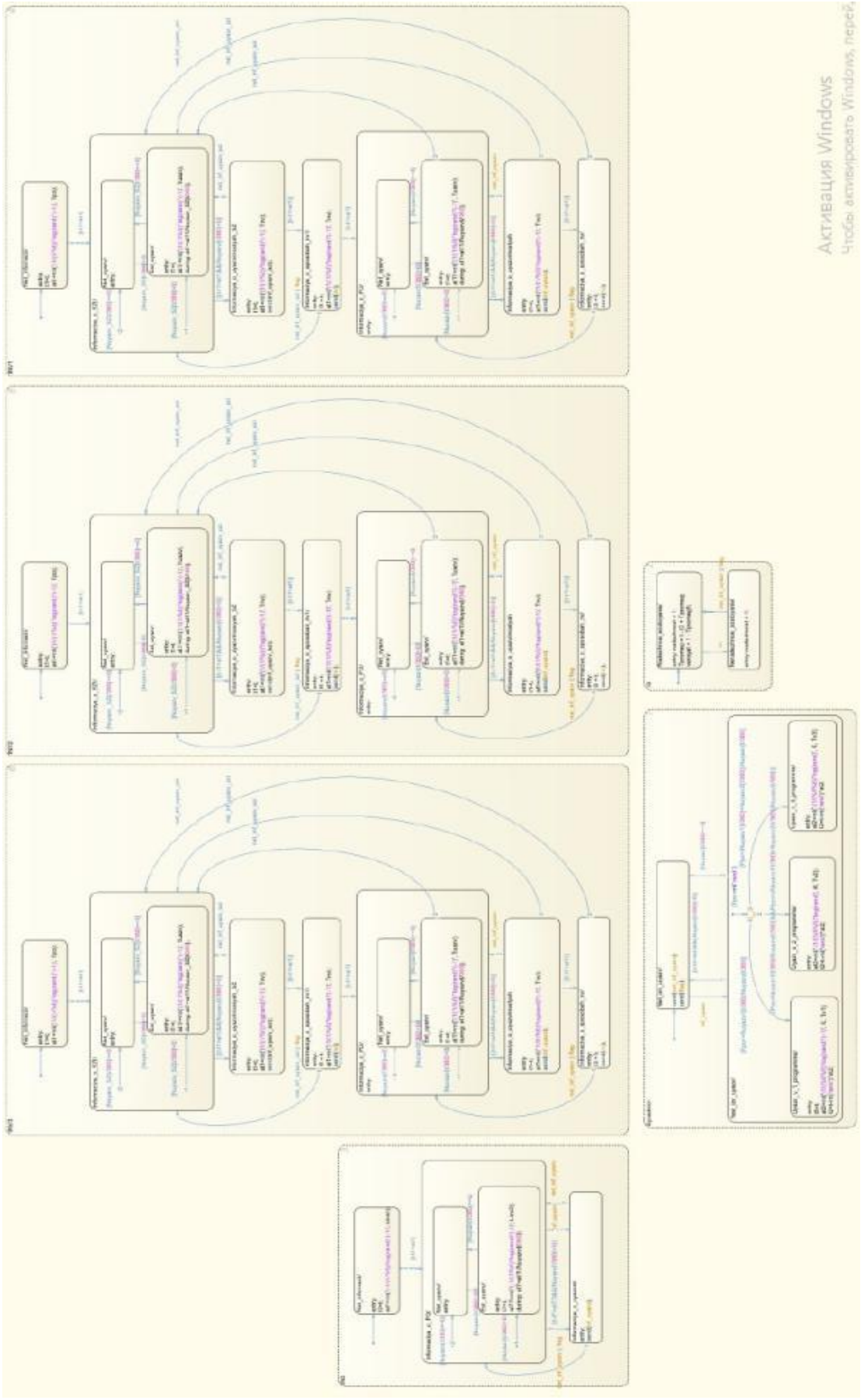


Рисунок 4.13 – Загальна імітаційна модель типового конфлікту

5 ВИСНОВКИ

Запропоновано математичні та об’єктно-орієнтовані моделі динаміки станів інформаційної системи з урахуванням можливих різних складових характеристик, а також характеристик дефектів, що враховують залежності інтенсивностей знаходження вразливостей від таких факторів як: час, часові характеристики закриття вразливостей, робота вендорів, адміністраторів інформаційної системи, наявність інсайдера або коаліції джерел негативного впливу.

Математичні та об’єктно-орієнтовані моделі конфліктів інформаційної системи та джерел негативного впливу дозволяють враховувати різний склад і структуру інформаційної системи (наявність різного програмного забезпечення, наявність засобів захисту інформації тощо), динаміку і кількість вразливостей в інформаційній системі, а також вплив на надійність системи роботи системного адміністратора і вендорів.

Розроблено інформаційну технологію аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів, яка враховує динаміку зміни вразливостей, а також ряд параметрів, що визначають ситуаційний характер конфліктної взаємодії сторін.

На відміну від існуючих інтуїтивних підходів до аналізу вразливостей, розроблена модель побудована за принципом імітації процесу зміни станів системи, який залежить від організаційно-технічних характеристик системи забезпечення надійності. Дана імітаційна модель ситуаційного конфлікту інформаційної системи і джерел негативного впливу дозволяє приймати обгрунтовані рішення з питань забезпечення надійності.

За допомогою результатів можна:

– юзерам інформаційних систем – виявляти «узькі» місця в політиці забезпечення надійності, оцінювати матеріальні та інші ризики, а також виробляти поради щодо їх зменшення;

– розробникам програмного забезпечення – оптимально розподілити грошові та будь-які ресурси, що стосуються розробки нових програмних продуктів та підтримки вже існуючих.

6 СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. G´eraldine Vache Marconato Security-related vul-nerability life cycle analysis / G´eraldine Vache Marconato, Vincent Nicomette, Mohamed Kaˆaniche // 7th International Conference on Risk and Security of Internetand Systems (CRiSIS-2012), 2012. pp. 1–8.

2. Joh, H. Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics / H. Joh, Y.K. Malaiya // SAM'11, The 2011 International Conference on Security and Management, 2011. pp.10-16.

3. Okamura, H. Tokuzane H., Dohi T. Quantitative Security Evaluation for Software System from Vulnerability Database / H. Okamura, M. Tokuzane, T. Dohi // Journal of Software Engineering and Applications, Vol. 6 No. 4A, 2013. pp. 15-23.

4. Щербань Т. Інформаційні системи і зовнішні негативні впливи на них // Перший крок у науку, м.Суми, 24 лютого 2019 р.–Суми:СумДУ, 2019.–с.23

5. How to Find Security Vulnerabilities // URL: https://www.compuquip.com/blog/how-to-find-security-vulnerabilities

6. The Ultimate security vulnerability datasource // CVE Details. URL: https://www.cvedetails.com/vendor/26/Microsoft.html

7. National Vulnerability Database // National Institute of Standards and Technology. URL: http://nvd.nist.gov

8. Microsoft Security Intelligence Report v19 // Mictosoft. URL: http://www.microsoft.com/security/sir/.

9. The Anatomy of an Anonymous Attack, Hacker Intelligence Summary Report // Imperva. URL: http://www.imperva.com/docs/hii_the_anatomy_ of_an_anonymous_attack.pdf.

10. ЩербаньТ., Кіншаков Е., Лавров Е.А. Аналіз проблем людського фактору в задачах забезпечення кібербезпеки// Інформатика, математика, автоматика: матеріали та програма науково-технічної конференції, м. Суми, 5-9 лютого 2018 р. – Суми : СумДУ, 2018. –С. 95-96

11. Застрожнов, І.І. Модель конфлікту зловмисника і системи захисту інформації / І.І. Застрожнов, Д.І. Коробкин, А.А. Окрачков, Е.А. Рогозин. Вісник Воронезького державного технічного університету. 2009. Т. 5. № 6. С. 142-149.

12. Етичний взлом в Інтернеті // URL: https://swsu.ru/sbornik-statey/ethical-hacking-on-the-internet.php

13. Безпека інформаційних систем // URL: http://intuit.valrkl.ru/course-1312/index.ht

14. Нестеров, С. Аналіз і управління ризиками в інформаційних системах на базі операційних систем Microsoft / С. Нестеров. URL: http://www.intuit.ru/studies/courses/531/387/info.

15. Вялих, А.С. Оцінка можливостей атаки на інформаційну систему / Вялих А.С., Вялих С.А. // Кібернетика і високі технології XXI століття: матер. XII міжнарод. наук.-тех. конф., Воронеж, 11-12 травня 2011 г. Воронеж: ІСЦ ВДУ, 2011. Т.1. С. 91-96.

16. Кіншаков Е.,Щербань Т., Аналіз задач забезпечення кібербезпеки//«Інтелектуальний потенціал – 2018» - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя підготовки ІТ- фахівців ХНУ/ Колектив авторів – Хмельницький: ПВНЗ УЕП, 2018. – Ч.3: Кібербезпека та актуальні проблеми комп’ютерних систем і мереж – С.50-51

17. Ліпаєв, В.В. Надійність програмного забезпечення / В.В. Ліпаєв М.: Радіо і зв’язок, 1998. 200 с.

18. Shooman, M.L. Software Engineering: Reliability, Development and Management / M.L. Shooman // N.Y. McGraw-Hill. 1983.

19. Щеглов, А.Ю. Безпека сучасних ОС «у цифрах» / А. Ю. Щеглов. URL: http://www.itsec.ru/articles2/Inf_security/bezopasnost-OS.

20. Shooman, M.L. Software Engineering: Reliability, Development and Management / M.L. Shooman // N.Y. McGraw-Hill.

21. Застрожнов, І.І. Модель конфлікту зловмисника і системи захисту інформації / І.І. Застрожнов, Д.І. Коробкин, А.А. Окрачков, Е.А. Рогозин. Вісник Воронезького державного технічного університету. 2009. Т. 5. № 6. С. 142-149. 31.

22. Клімов, І. З. Оцінка надійності систем захисту інформації від несанкціонованого доступу / І. З. Клімов, А. А. Пономарьов. Вісник Іжевського державного технічного університету. 2008. №-3. С. 102-103.

23. Stochastics An International Journal of Probability and Stochastic Processes, Volume 92, Issue 8 (2020)

24. Шелухін, О. І. Виявлення вторгнень в комп'ютерні мережі [мережеві аномалії] / О. І. Шелухін, Д. Ж. Сакалема, А. С. Філінова. М .: Гаряча лінія Телеком, 2013. 220 с.

25. GantPRO // URL: https://app.ganttpro.com/

26. Draw.io. URL: https://app.diagrams.net/

27. Simulink Basics Tutorial. URL: https://eelabs.faculty.unlv.edu/docs/guides/Simulink_Basics_Tutorial.pdf

28. Simulink and Stateflow tutorials. URL: https://linklab-uva.github.io/modeling_cps/files/resources/simulink.pdf

29. Introduction to Stateflow. URL: https://meta-guide.com/videography/100-best-matlab-stateflow-videos

30. Методологія функціонального моделювання IDF0. URL: https://nsu.ru/smk/files/idef.pdf

31. Вялих, А.С. Оцінка можливостей атаки на інформаційну систему / Вялих А.С., Вялих С.А. // Кібернетика і високі технології XXI століття: матер. XII міжнарод. наук.-тех. конф., Воронеж, 11-12 травня 2011 г. Воронеж: ІСЦ ВДУ, 2011. Т.1. С. 91-96.

32. Кельберт, М. Я. Статистика та ймовірність в задачах та прикладах. Т. II: Ланцюги Маркова як відправна точка теорії випадкових процесів та їх застосування / М.Я. Кельберт, Ю.М. Сухов, 2009. 295 с.

33. The Anatomy of an Anonymous Attack, Hacker Intelligence Summary Report // Imperva. URL: http://www.imperva.com/docs/hii_the_anatomy_of_an_ anonymous_attack.pdf.

34. Ethical Hacking and Countermeasures: Attack Phases / M. Bellegarde, M. Orvis, S. Helba. EC-Council Press, 2010.

35. UML Diagram. . URL: https://www.smartdraw.com/uml-diagram/

36. Алгазінов, Є.К. Комп’ютерне моделювання та аналіз інформаційних систем і процесів / Е. К. Алгазінов, 2009. 416 с.

37. Постановка цілей по SMART. URL: https://goal-life.com/uk/smart-cil

38. SMART цілі і завдання в прикладах. URL: https://equity.today/chto-takoe-zadachi-smart-i-kak-oni-rabotayut.html

39. Лукацкий А.В. Виявлення вразливостей комп'ютерних мереж. URL: http://www.citforum.ru/security/internet/vulnerability/

40. Кучер В.А., Агранович В.С. Використання методів теорії ймовірностей і математичної статистики для оцінки ймовірностей виявлення вразливостей в інформаційних автоматизованих системах. URL: www.contrterror.tsure.ru/site/magazine5/pdf/06-38-K.ucher-Agranovich.pdf.

41. Бейс Ребекка. ICSA. Введение в обнаружение атак и анализ защищенности. URL: : http://bugtraq.ru/library/books/icsa/index.html

42. Щеглов А. Вразливості сучасних ОС. URL: http://www.cnews.ru/reviews/free/security2005/articles/vulnerability.shtml

43. Боровко Р. Число вразливостей в програмному забезпеченні різко скорочується. URL: http://www.cnews.ru/reviews/free/security2004/globalthreats /index2.shtml

44. Структура декомпозиції робіт WBS. URL: https://www.cfin.ru/itm/project/wbs.shtml

45. Методології, які використовуються в bPwin. URL: https://studfiles.net/preview/5609405/page:3/

46. Бюджетування проекту. URL: https://pidruchniki.com/87726/menedzhment/byudzhetuvannya_proektu

47. Моделювання бізнес-процесів з BPwin 4.0. URL: https://it.wikireading.ru/35221

48. Жуковський М. Є. Основи теорії випадкових процесів / М. Є. Жуковський, І. В. Родіонов, Д. А. Шабанов., 2016. – 121с.

49. Каштанов В. А. Випадкові процеси: підручник і практикум для прикладного бакалаврату / В. А. Каштанов. – Москва: Юрайт, 2019. – 156 с.

50. Круглов В. М. Випадкові процеси в 2 ч. Частина 1. Основи загальної теорії: підручник для вузів / В. М. Круглов. – Москва: Юрайт, 2020. – 276 с.

51. Єнацька Н. Ю. Математична статистика і випадкові процеси / Н. Ю. Єнацька. – Москва: Юрайт, 2020. – 201 с.

52. Фаулер, М. UML. Основи. 2-е вид. Короткий посібник ПЗ уніфікованої мови моделювання / М. Фаулер, К. Скотт .: Пер. з англ. СПб .: Видавництво: «Символ-Плюс», 2006. 192с.

53. Потєхін В.С., Родін В.Н., Чудаков О.Е. Програмування: мови, методи, технології. Ч.1. Технології розробки програмного забезпечення: навчальний посібник / В.С. Потєхін, В.Н. Родіонов, О.Е. Чудаков, 2015. – 132с.

ДОДАТОК А ПЛАНУВАННЯ РОБІТ

А.1 Ідентифікація мети проекту

Розвиток використовуваних інформаційних технологій, ускладнення завдань, які виконуються сучасними інформаційними системами вимагає все більш оновлених підходів до аналізу та оцінювання надійності інформаційної системи. Підходи, які використовуються, не враховують випадкового характеру факторів, що впливають на надійність інформаційної системи, не враховують динаміки окремих процесів, що впливають на надійність інформаційної системи, і динаміки конфлікту між різними суб’єктами, які беруть участь в цих процесах, не враховують доступність джерел даних для оцінки параметрів, що впливають на надійність інформаційної системи, і реалізацію моделей та алгоритмів прогнозування цих даних.

Метою є оптимізація та розробка математичних, об’єктно-орієнтованих моделей, та на їх основі – імітаційної, для аналізу надійності використання програмного забезпечення в інформаційних системах в умовах конфліктних взаємодій з урахуванням ряду важливих ймовірністних характеристик конфлікту.

Узагальнений вигляд мети полягає у вивченні процесу функціонування інформаційної системи при наявності в в її програмному забезпечені джерела негативного впливу, а також аналізу надійності інформаційної системи в майбутньому.

А.2 Деталізація мети методом SMART

Метод SMART часто використовується для деталізації мети, який дозволяє визначати цілі та поставити завдання в менеджменті та управлінні проектами.

Сутність деталізації мети проекту за допомогою SMART-методу випливає з розшифровки термінів, які формують його назву [37,38]:

- конкретна мета (Specific),
- вимірювана (Measurable),
- досяжна (Achievable),
- реалістична (Relevant),
- обмежена у часі (Time-framed).

Результати деталізації представлені у таблиці А.1

Таблиця А.1 – Деталізація мети методом SMART

Specific (конкретна)	Оптимізувати математичні, об’єктно-орієнтовані та імітаційні моделі конфлікту «інформаційна система – джерело негативного впливу» з урахуванням ряду важливих ймовірністних характеристик конфлікту.
Measurable (вимірювана)	Результат – математичні, об’єктно-орієнтовані та імітаційні моделі, за допомогою яках можна виконувати аналіз надійності використання програмного забезпечення в інформаційній системі в умовах конфліктних взаємодій з урахуванням ряду важливих ймовірністних характеристик конфлікту.
Achievable (досяжна)	Для того, щоб мета була досягнута, необхідно розробити – математичні, об’єктно-орієнтовані та імітаційні моделі конфлікту інформаційної системи з джерелом негативного впливу з урахуванням ряду важливих ймовірністних характеристик конфлікту.
Relevant (реалістична)	У наявності є всі необхідні технічні та програмні засоби. Розробники мають достатній рівень знань для виконання поставлених задач.

Продовження таблиці А.1

Time-framed (обмежена у часі)	Ціль має часове обмеження. Робота повинна бути виконана у терміни, що були оговорені керівником проекту із замовником.

Даний аналіз, проведений методом SMART дозволив визначити кінцеву мету: створення математичної, об’єктно-орієнтованих та імітаційної моделей використання програмного забезпечення в інформаційній системі в умовах конфліктних взаємодій до 1 грудня 2020 року.

А.3 Дослідження продукту ІТ-проекту, організації, ринку, регіону

Автоматизація будь-якої організаційної системи несе з собою не тільки відомі переваги, які стимулюють весь процес інформатизації, але і появу нових загроз, пов’язаних з використанням інформаційних автоматизованих систем. Однак загрози самі по собі не проявляються, всі загрози можуть бути реалізовані при наявності активних суб’єктів – джерел негативного впливу та, власне, слабких місць – вразливостей, притаманних окремим компонентам інформаційних автоматизованих систем [39].

Проблема вразливостей вивчається давно і відкрито. Розроблена велика кількість методик та підходів до аналізу захищеності. Описане використання методів теорії ймовірності та математичної статистики для оцінки ймовірностей виявлення вразливостей в інформаційних автоматизованих системах [40], видано серії книг, присвячених системам виявлення атак [41].

На думку одних авторів, статистика показує, що кількість вразливостей зростає рік від року. З одного боку, це пов'язано з тим, з кожним роком зростає кількість програмного забезпечення, а з іншого – з тим, що зараз вразливості шукаються навмисно як хакерами, так і компаніями-виробниками програмного забезпечення і

операційних систем [42]. На думку інших, криза на IT-ринку, викликана зростанням злому комп'ютерних систем і окремих програмних забезпечень (а як наслідок – економічний збиток від неуваги до питань інформаційної безпеки ріс космічними темпами), привів до того, що замовники перестали постійно «оновлювати» програмне забезпечення, оскільки, крім косметичних нововведень, в продуктах не було реальних поліпшень. Скорочення замовлень змусило розробників переорієнтуватися з косметичної на більш детальне доопрацювання своїх продуктів. Отже, завдяки цьому, число вразливостей в програмних забезпеченнях стало різко скорочуватися[43].

Виходячи з цього, запропоновані оптимізовані математичні та об’єктно-орієнтовані моделі динаміки станів програм і інформаційної системи з урахуванням ряду можливих ймовірнісних факторів вразливостей, що враховують залежності інтенсивностей виявлення вразливостей від часу, часових характеристик закриття вразливостей від роботи виробника програмного забезпечення і адміністратора інформаційної системи, кількості вразливостей, наявності засобів захисту інформації, а також наявності інсайдера. На основі моделей була розроблена та потім удосконалена імітаційна модель аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів.

Отримані результати дозволяють:

– для користувачів інформаційних систем – виявляти слабкі місця в політиці забезпечення надійності, виявити програмне забезпечення використання якого небажано, оцінити кваліфікацію системного адміністратора, дати оцінку матеріальним та іншим ризикам, яким може піддатися інформаційна система, а також розробити рекомендації, як їх зменшити;

– для розробників програмного забезпечення – раціонально розпоряджатися як фінансовими так і іншими ресурсами щодо підтримки існуючого програмного забезпечення та розробці нового;

– для організацій, що здійснюють атестацію інформаційних систем і сертифікацію програмного забезпечення – точніше оцінювати реальні процеси

функціонування інформаційних систем в умовах конфліктних взаємодій, виробити на основі розроблених моделей і алгоритмів нову методологію, яка буде більш повно враховувати дані процеси.

А.4 Попередній опис змісту проекту

Нижче наведений попередній перелік пунктів змісту проекту:

– характеристика проблеми забезпечення надійності інформаційних технологій та систем при наявності внутрішніх вразливостей;

– аналіз ймовірнісних характеристик негативного впливу в сучасних інформаційних системах;

– загальний алгоритм аналізу ймовірністних характеристик наявності джерел негативного впливу в програмному забезпеченні;

– математична модель функціонування інформаційної системи з наявними засобами захисту інформації;

– математична модель функціонування інформаційної системи з коаліцією джерел негативного впливу;

– математична модель функціонування інформаційної системи з інсайдером;

– об’єктно-орієнтована модель функціонування інформаційної системи з наявними засобами захисту інформації;

– об’єктно-орієнтована модель функціонування інформаційної системи з коаліцією джерел негативного впливу;

– об’єктно-орієнтована модель функціонування інформаційної системи з інсайдером;

– порівняння імітаційних результатів;

– імітація ряду типових ситуацій.

А.5 Формалізація мети продукту та результату проекту

Формалізація мети роботи полягає у розробці моделі і алгоритму аналізу та прогнозування надійності використання програмного забезпечення в інформаційних системах в умовах конфліктних взаємодій.

Для виконання даної роботи необхідно вирішити наступні задачі:

– аналіз найбільш важливих факторів, що впливають на надійність використання програмному забезпеченні в інформаційній системі;

– визначення основних вимог до розроблюваних алгоритмів і моделей аналізу надійності використання програмного забезпечення в інформаційній системі в умовах конфліктних взаємодій;

– аналіз сучасних підходів до оцінки надійності використання програмного забезпечення в інформаційній системі на предмет врахування даних факторів і вимог;

– розробка моделей функціонування інформаційних систем при наявності внутрішніх вразливостей;

– розробка алгоритмів і моделей оцінки надійності використання програмного забезпечення в інформаційній системі в умовах конфліктних взаємодій, які враховують найбільш важливі фактори і відповідають основним вимогам, визначеним раніше.

Об’єкт дослідження. Конфліктні взаємодії в інформаційних системах.

Предмет дослідження. Модель інформаційної системи в умовах конфліктних взаємодій.

Продуктом даного проекту є математична, об’єктно-орієнтовані та імітаційна моделі конфлікту програмного забезпечення в інформаційній системі та джерела негативного впливу.

А.6 Планування змісту структури робіт

Структура декомпозиції робіт (WBS) визначає зміст проекту і будується виходячи з основних цілей проекту. кожен рівень ієрархії відображає більш детальне визначення компонентів проекту. Ієрархічна структура декомпозиції робіт допомагає оцінити проміжні та кінцеві результати: вартість і час, на різних етапах проекту. WBS є схемою проекту, за допомогою якого керівник проекту завжди може визначити, чи всі проміжні точні результати, що ведуть до досягнення мети проекту, враховані[44].

Створена WBS-діаграма представлена на рисунку А.1.

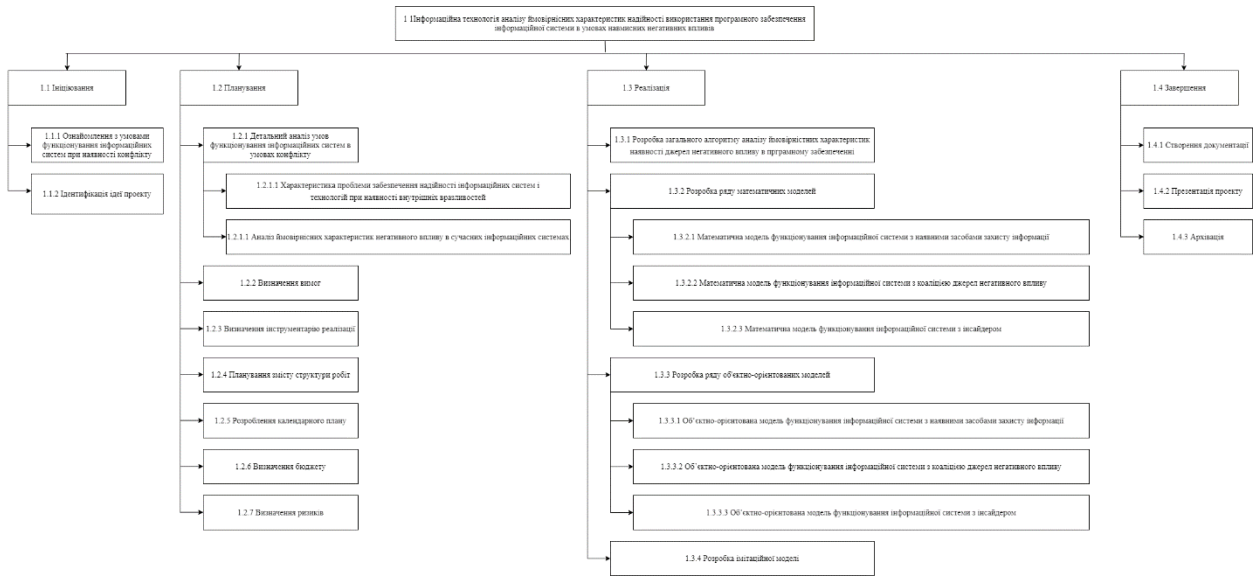


Рисунок А.1 – WBS структура проекту

А.7 Планування структури виконавців

Організаційна структура проекту (Organization Breakdown Structure OBS) представляє собою діаграму, яка за своєю структурою відповідає WBS-діаграмі, з тою різницею, що замість робіт, які повинні бути виконані, елементами схеми є виконавці

даних робіт. Вона є ієрархічною структурою управління проектом і показує відносини між учасниками проекту[45].

У проекті створена та автоматизована інформаційна технологія конфлікту інформаційної системи з джерелом негативного впливу:

– студент Щербань Тетяна Володимирівна – розробник;

– професор Лавров Євгеній Анатолійович – керівник проекту;

Графічне представлення OBS-діаграми, що була створена для даного проекту показане на рисунку А.2.

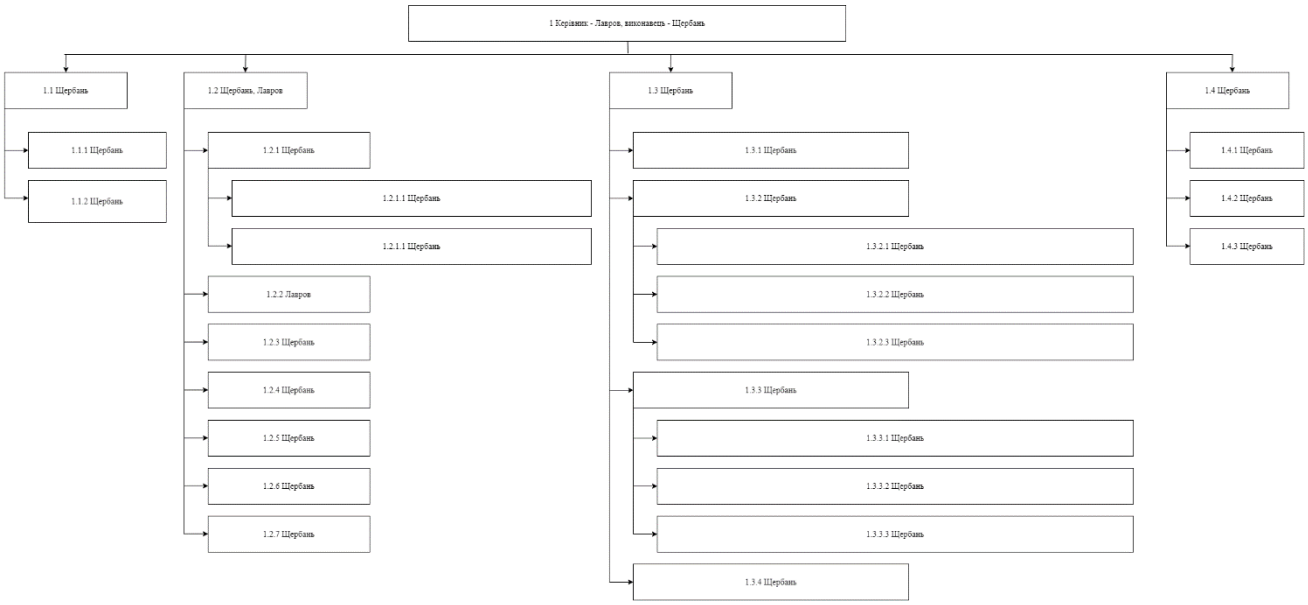


Рисунок А.2 – OBS структура

А.8 Побудова матриці відповідальності

На підставі OBS та WBS структур було побудовано матрицю відповідальності. Для кожного із виконавців була визначена його роль.

На рисунку А.3 показано матрицю відповідальності проекту.

	CP1																					
	CP1.1		CP1.2								CP1.3								CP1.4			
	CP1.1.1	CP1.1.2	CP1.2.1		CP1.2.2	CP1.2.3	CP1.2.4	CP1.2.5	CP1.2.6	CP1.2.7	CP1.3.1	CP1.3.2			CP1.3.3			CP1.3.4	CP1.4.1	CP1.4.2	CP1.4.3	
			CP1.2.1.1	CP1.2.1.2								CP1.3.2.1	CP1.3.2.2	CP1.3.2.3	CP1.3.3.1	CP1.3.3.2	CP1.3.3.3					
Лавров Є.А.					+																	
Щербань Т.В.	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Рисунок А.3 – Матриця відповідальності

А.9 Побудова календарного графіку виконання проекту

Найпоширеніший формат графіка проекту в будь-якій галузі – це діаграма Ганта, названа на честь його розробника, інженера-механіка і консультанта з питань управління Генрі Ганта. Цей графік в графічній формі дозволяє менеджерам проекту і всій команді розробників візуалізувати графіки часу і взаємозв'язок між окремими завданнями та етапами роботи над проектом. Його можна створити вручну або за допомогою комп'ютерної програми, але в будь-якому випадку його основою виступають дані для конкретного проекту.

Тривалість виконання робіт була зазначена в днях, але фактична тривалість виконання робіт приблизно дорівнює 2 години на день.

Основні сумарні задачі, весь список робіт та діаграма Ганта приведені на рисунках А.4-А.5.

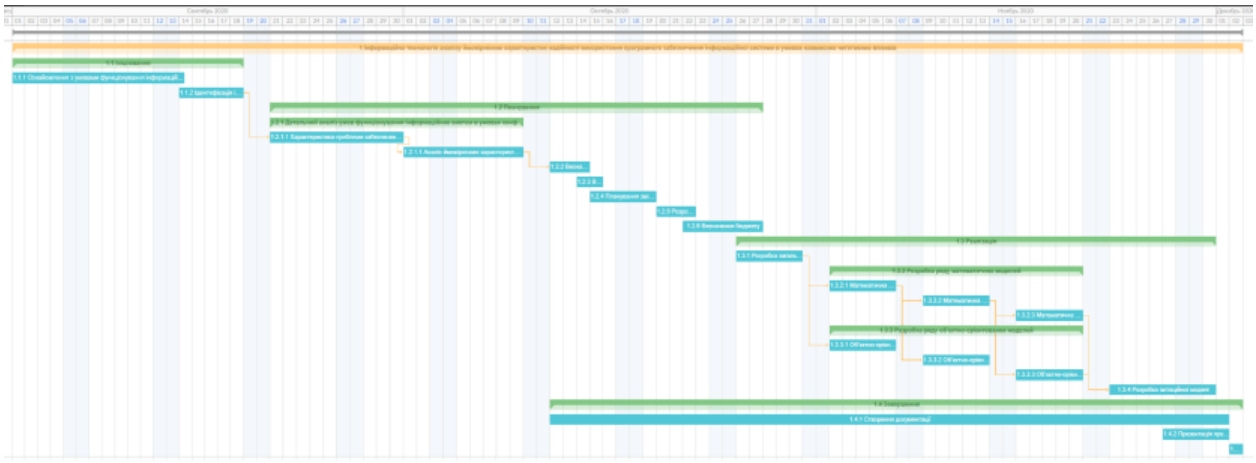


Рисунок А.4 – Діаграма Ганта

Задача	Начало	Завершение
	01.09.2020	**02.12.2020**
1 Інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів	**01.09.2020**	**02.12.2020**
1.1 Ініціювання	**01.09.2020**	**18.09.2020**
1.1.1 Ознайомлення з умовами функціонування інформаційних систем при наявності конфлікту	01.09.2020	14.09.2020
1.1.2 Ідентифікація ідеї проекту	14.09.2020	18.09.2020
1.2 Планування	**21.09.2020**	**27.10.2020**
1.2.1 Детальний аналіз умов функціонування інформаційних систем в умовах конфлікту	**21.09.2020**	**09.10.2020**
1.2.1.1 Характеристика проблеми забезпечення надійності інформаційних систем і технологій при наявності внутрішніх вразливостей	21.09.2020	30.09.2020
1.2.1.1 Аналіз ймовірнісних характеристик негативного впливу в сучасних інформаційних системах	01.10.2020	09.10.2020
1.2.2 Визначення вимог	12.10.2020	14.10.2020
1.2.3 Визначення інструментарію реалізації	14.10.2020	15.10.2020
1.2.4 Планування змісту структури робіт	15.10.2020	19.10.2020
1.2.5 Розроблення календарного плану	20.10.2020	22.10.2020
1.2.6 Визначення бюджету	22.10.2020	27.10.2020
1.3 Реалізація	**26.10.2020**	**30.11.2020**
1.3.1 Розробка загального алгоритму аналізу ймовірністних характеристик наявності джерел негативного впливу в прграмному забезпеченні	26.10.2020	30.10.2020
1.3.2 Розробка ряду математичних моделей	**02.11.2020**	**20.11.2020**
1.3.2.1 Математична модель функціонування інформаційної системи з наявними засобами захисту інформації	02.11.2020	06.11.2020
1.3.2.2 Математична модель функціонування інформаційної системи з коаліцією джерел негативного впливу	09.11.2020	13.11.2020
1.3.2.3 Математична модель функціонування інформаційної системи з інсайдером	16.11.2020	20.11.2020
1.3.3 Розробка ряду об'єктно-орієнтованих моделей	**02.11.2020**	**20.11.2020**
1.3.3.1 Об'єктно-орієнтована модель функціонування інформаційної системи з наявними засобами захисту інформації	02.11.2020	06.11.2020
1.3.3.2 Об'єктно-орієнтована модель функціонування інформаційної системи з коаліцією джерел негативного впливу	09.11.2020	13.11.2020
1.3.3.3 Об'єктно-орієнтована модель функціонування інформаційної системи з інсайдером	16.11.2020	20.11.2020
1.3.4 Розробка імітаційної моделі	23.11.2020	30.11.2020
1.4 Завершення	**12.10.2020**	**02.12.2020**
1.4.1 Створення документації	12.10.2020	01.12.2020
1.4.2 Презентація проекту	27.11.2020	01.12.2020
1.4.3 Архівація	02.12.2020	02.12.2020

Рисунок А.5 – Весь список робіт для побудови діаграми

А.10 Планування ризиків проекту

На перший погляд, створення досить детального плану проекту, оптимізованого за термінами і витратами, позбавляє менеджера проекту від будь-яких проблем аж до настання дати завершення проекту. Однак в реальному житті трапляються події, здатні негативно вплинути на хід проекту. Подібні події, які важко передбачити заздалегідь, але які здатні негативно вплинути на хід реалізації проекту, зазвичай називають ризиками. У контексті проекту ризик – це ймовірність настання небажаної події та всіх його можливих наслідків. При настанні будь-якого з них з'являється небезпека не завершити проект вчасно, не вкластися в бюджет, не виконати умови контракту і т.д.

Для того, щоб передбачити різні негативні фактори та небезпеки, які можуть трапитись під час виконання та експлуатації проекту та максимально його захистити, необхідно розробити завчасно продуману стратегію управління ризиками[46].

Як правило, в управлінні ризиками розрізняють наступні етапи:

– ідентифікація ризиків;
– кількісна і якісна оцінка ризиків;
– розробка стратегії мінімізації витрат через ризики.

Діаграма ризиків, визначення основних ризиків проекту, варіанти запобігання ризиків та реакції на ризики показані на рисунку А.6 та у таблицях А.2-А.3.

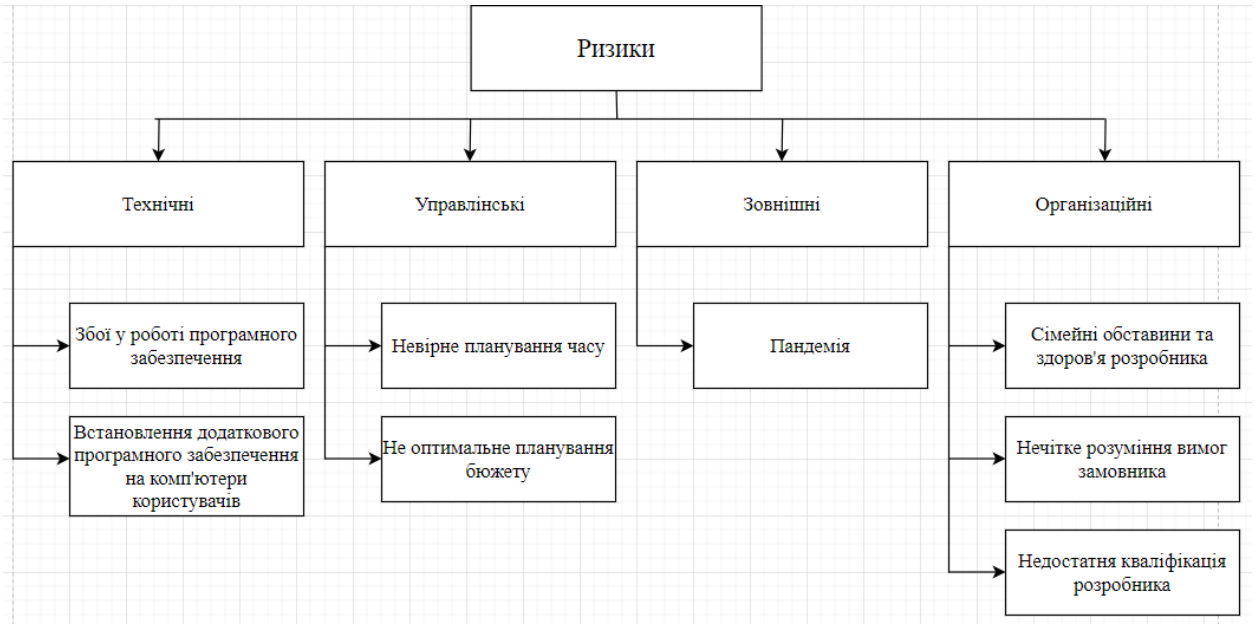


Рисунок А.6 – Діаграма ризиків проекту

Нижче представлена таблиця визначення характеристик ризиків проекту, де ймовірність буде визначена значенням від 0 до 1, де 0 – найменша вірогідність, а 1 – найбільша. Втрати та вплив визначені значеннями від 0 до 5, де 0 – найменше значення і відповідно 5 – найбільше. Характер ризиків представленний переліком варіантів: незначний, помірний або ж значний вплив являє даний ризик на успішність реалізації проекту.

Таблиця А.2– Визначення характеристик ризиків

Назва	Імовірність	Втрати	Вплив	Характер
Пандемія	0.8	2	2	Помірні
Невірне планування часу	0.3	5	5	Значні
Недостатня кваліфікація розробника	0.3	3	3	Незначні
Сімейні обставини та здоров’я розробника	0.4	2	4	Помірні
Збої у роботі програмного забезпечення	0.2	2	3	Незначні
Не оптимальне планування бюджету	0.4	4	4	Значні
Встановлення додаткового програмного забезпечення на комп’ютери користувачів	0.6	3	1	Незначні
Нечітке розуміння вимог замовника	0.7	5	5	Значні

Нижче в таблиці А.3 представлені варіанти запобігання ризиків та реакції на ризики, що були перераховані вище.

Таблиця А.3 – Варіанти запобігання ризиків та реакції на ризики

Ризики проекту	План запобігання ризику	Мінімізація наслідків
Пандемія	Завчасно призначити та запланувати усі можливі заходи з дотриманням усіх визначених вимог	Перевести усі зустрічі у онлайн формат, надати усю необхідну інформацію розробнику та вести чат-контроль процесу розробки проекту
Невірне планування часу	Оптимізувати розподіл часу виконаня проекту	Намагатися раціонально використати час, що залишився, розставити приорітети та діяти згідно з планом
Недостатня кваліфікація розробника	Завчасно ознайомити розробника з використовуваними технологіями	Виділити деяку кількість днів на ознайомлення з технологіями та інструментами проекту

Продовження таблиці А.3

Сімейні обставини та здоров’я розробника	Зарезервувати деяку конкретну кількість днів на на можливі відпустки/лікарняні/інші обставини, що відносяться до людського фактору	При плануванні термінів робіт додатково виділяти декілька днів на можливість використання розробником зарезервованих днів
Збої у роботі програмного забезпечення	Використувати стабільні версії інструментів, необхідних для проекту	Використувати стабільні версії інструментів, необхідних для проекту
Не оптимальне планування бюджету	Своєчасна перевірка кошторисів	Компенсувати втрати за рахунок інших етапів проекту
Встановлення додаткового програмного забезпечення на комп’ютери користувачів	Планування інтеграції даної технології у незалежний програмний додаток	Адаптивність та сумісність розроблюваних моделей з портативними версіями необхідного додатка
Нечітке розуміння вимог замовника	Вчасно знайти невідповідність та обговоривши з замовником внести необхідні правки	Знайти дистанційний спосіб комунікації, та виділити більше часу на обговорення деталей задачі проекту та його етапів

А.11 Формування бюджету проекту

Підготовка бюджету – це один з процесів управління проектами, який необхідний для того, щоб забезпечити розробку, обґрунтування та готовність до використання економічно ефективним чином.

Бюджетування проекту – це визначення вартості робіт, виконуваних у рамках проекту та процес формування на цій основі бюджету проекту, що містить

встановлений розподіл витрат за видами робіт, статтями витрат, за часом виконання робіт, за центрами витрат або з інших позицій.

Є дві основні причини того, чому важливо складання проектів бюджетів. По-перше, затверджений бюджет сприяє фінансуванню проекту. Друга причина полягає в тому, що, зіставляючи проект і фактичну вартість затвердженого бюджету, можна визначити, чи йде проект відповідно до плану.

Структура бюджету визначається планом рахунків вартісного обліку конкретного проекту. Далі бюджет IT-проекту розраховується як сумарна вартість годин затрачених на розробку проекту, також додаються ризики (до 20%) та вартість проекту [47].

Перелік робіт та планування бюджету представлені в таблиці А.4. Вартість виконання робіт визначалась з урахуванням середніх цін на ринку IT-послуг в Україні у 2020 році.

Таблиця А.4 – Опис робіт та планування бюджету

Задачі	**Час виконання (дні)**	**Оплата за день (грн)**	**Ціна**
План виконання проекту	4	250	1000
Загальний алгоритм аналізу ймовірністних характеристик наявності джерел негативного впливу в програмному забезпеченні	2	250	1250
Математична модель функціонування інформаційної системи з наявними засобами захисту інформації	5	250	1250
Математична модель функціонування інформаційної системи з коаліцією джерел негативного впливу	5	250	1250

Продовження таблиці А.4

Математична модель функціонування інформаційної системи з інсайдером	5	250	1250
Об’єктно-орієнтована модель функціонування інформаційної системи з наявними засобами захисту інформації	5	250	1250
Об’єктно-орієнтована модель функціонування інформаційної системи з коаліцією джерел негативного впливу	5	250	1250
Об’єктно-орієнтована модель функціонування інформаційної системи з інсайдером	5	250	1250
Оптимізація імітаційної моделі	28	350	9800
Отримання та порівняння результатів моделі	5	300	1500
Створення документації	28	250	7000
Створення презентації	3	300	900
		Сума	28950

ДОДАТОК Б ТЕХНІЧНЕ ЗАВДАННЯ

ТЕХНІЧНЕ ЗАВДАННЯ

на створення математичної моделі, об’єктно-орієнтованих моделей та імітаційної моделі за темою«Інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів»

1 Найменування: інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів.

2 Терміни виконання: до 2 грудня 2020 року.

3 Призначення: на відміну від існуючих аналітичних моделей виявлення вразливостей запропоновані моделі зебезпечують представлення процесу появи і усунення вразливостей як напівмарківського процесу і опираються не лише на поточний стан інформаційної системи, але й дозволяють передбачити її надійність у майбутньому.

4 Мета: розробити інформаційну технологію аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів яка дозволяє врахувати динаміку зміни вразливостей, а також ряд інших параметрів, що визначають ситуаційний характер конфліктної взаємодії сторін.

5 Основні завдання: імітаційна модель ситуаційного конфлікту інформаційної системи і джерел негативного впливу дозволяє приймати обгрунтовані рішення з питань забезпечення надійності.

6 Вхідні дані: коефіцієнт діяльності системного адміністратора, середній час, необхідний джерелу негативного впливу для знаходження інформації про спосіб використання вразливості в програмному забезпеченні інформаційної системи для негативного впливу на інформаційну систему, середній час, необхідний джерелу негативного впливу для знаходження всіх вразливостей в інформаційній системі, середній час, необхідний джерелу негативного впливу для знаходження інформації про програмне забезпечення інформаційної системи.

7 Вихідні дані: графік ймовірності надійності інформаційної системи.

8 Програмне забезпечення: побудова напівмарківської моделі – Microsoft Visio 2016, розробка об’єктно-орієнтованих моделей – Visual Studio 2015, розробка імітаційної моделі – Matlab P2018 з бібліотеками Simulink та Stateflow.

9 Апаратне забезпечення: склад апаратного забезпечення повинен забезпечувати роботу програмного забезпечення, зазначеного у п. 8.

10 Рівень кваліфікації: користувач має володіти навичками роботи з ПК, та у програмному середовищі Matlab, вміти користуватись бібліотекою Simulink та Stateflow.

ДОДАТОК В ПРИКЛАДИ МОДЕЛЮВАННЯ

Розрахунок пропонується здійснити для джерел негативного впливу 4 різних рівнів кваліфікації:

– 1-ї категорії ($T_{ПЗ}$ = 60 днів, $T_{вразл}$ = 30 днів,$T_{нв}$ = 30 днів);

– 2-ї категорії ($T_{ПЗ}$ = 20 днів, $T_{вразл}$ = 30 днів,$T_{нв}$ = 10 днів);

– 3-й категорії ($T_{ПЗ}$ = 10 днів, $T_{вразл}$ = 5 днів,$T_{нв}$ = 5 днів);

– 4-ї категорії ($T_{ПЗ}$ = 5 днів, $T_{вразл}$ =1 день,$T_{нв}$ = 1 день).

Проведемо експерименти, щоб подивитися впливає кваліфікація адміністратора на ряд конфліктних взаємодій.

Позначимо, що коефіцієнт k пропонується оцінювати експертним шляхом:

– k=0, якщо адміністратор взагалі не встановлює патчі, що випущені вендором;

– k<1, якщо системний адміністратор не своєчасно встановлює патчі, випущені вендором;

– k=1, якщо адміністратор встановлює патчі одразу після їх випуску;

– k>1, якщо адміністратор встановлює патчі одразу після їх випуску і при цьому пропонує власну тимчасові рішення вирішення деяких вразливостей.

Нижче на рисунках В.1-В.4 представлено вірогідність надійності інформаційної системи при конфлікті з одним джерелом негативного впливу.

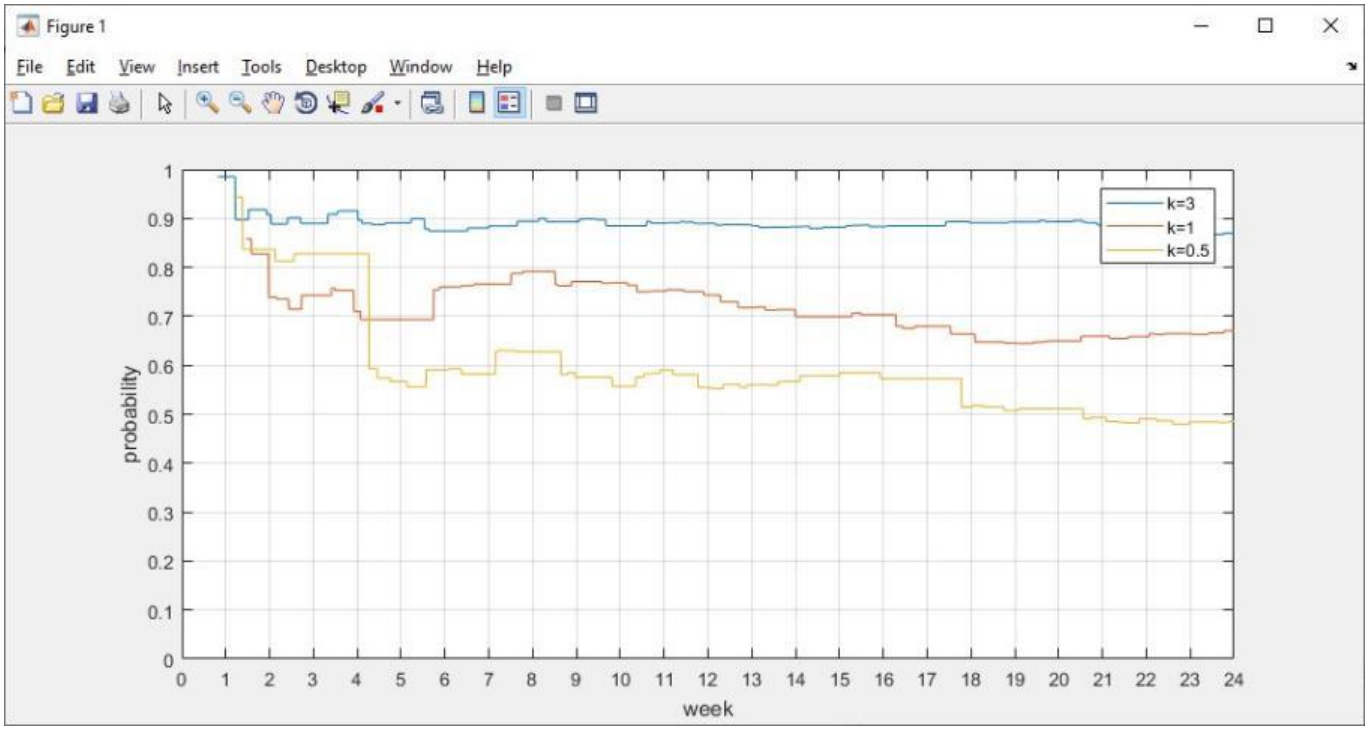


Рисунок В.1 – Вплив на систему джерела негативного впливу 1ї кваліфікації

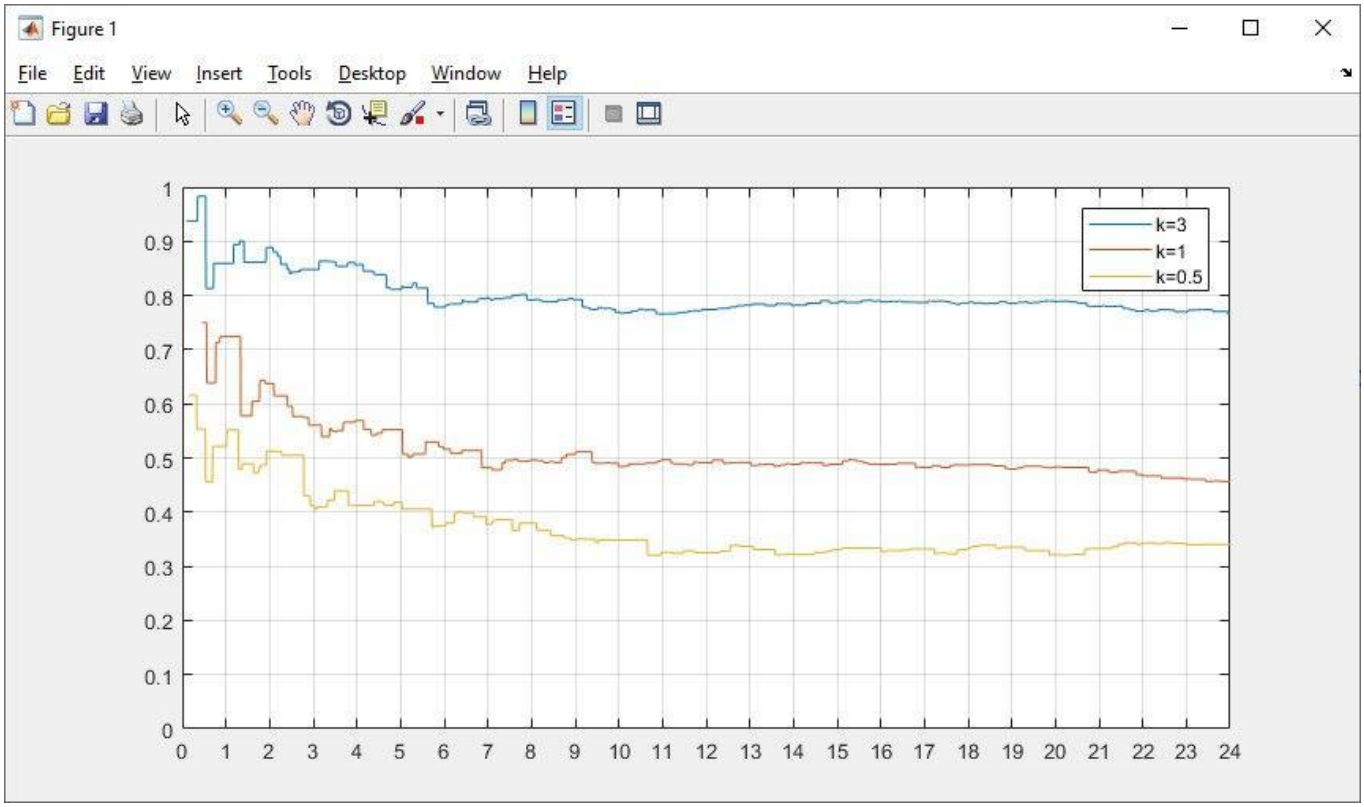


Рисунок В.2– Вплив на систему джерела негативного впливу 2ї кваліфікації

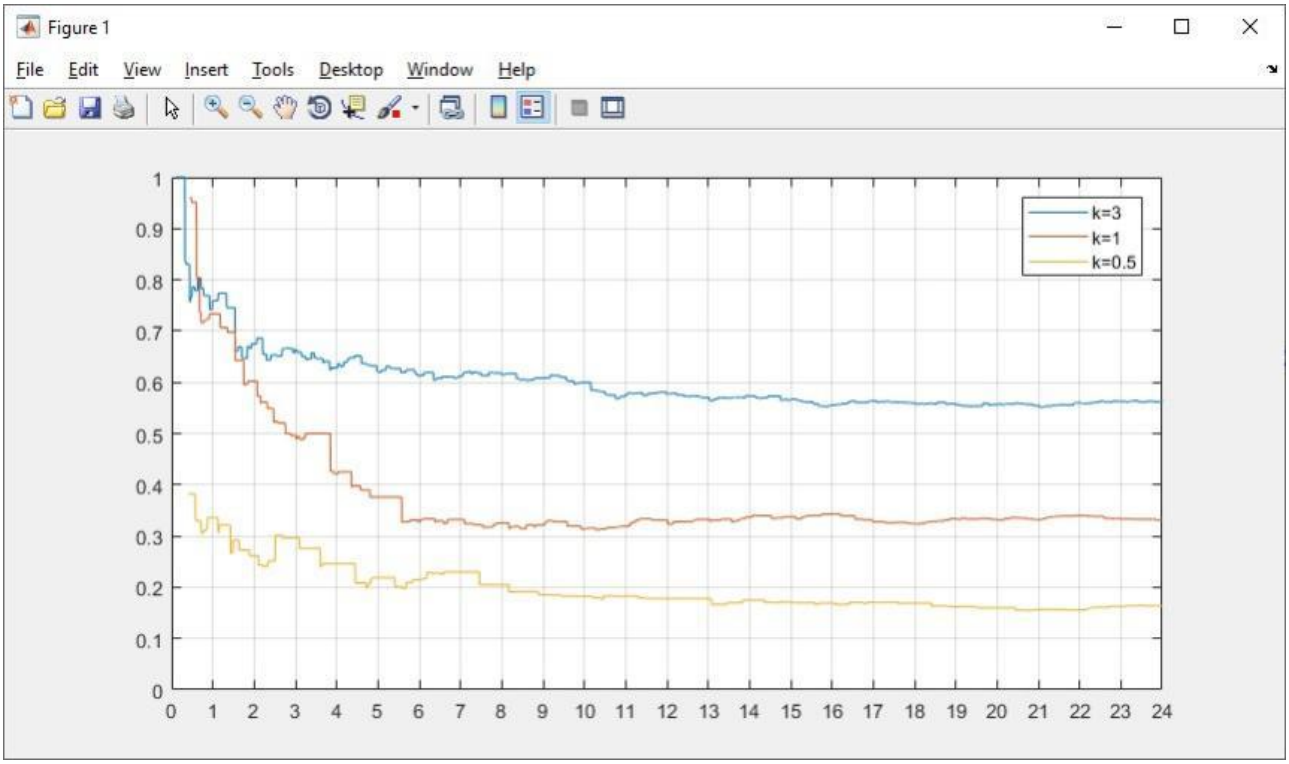


Рисунок В.3– Вплив на систему джерела негативного впливу 3ї кваліфікації

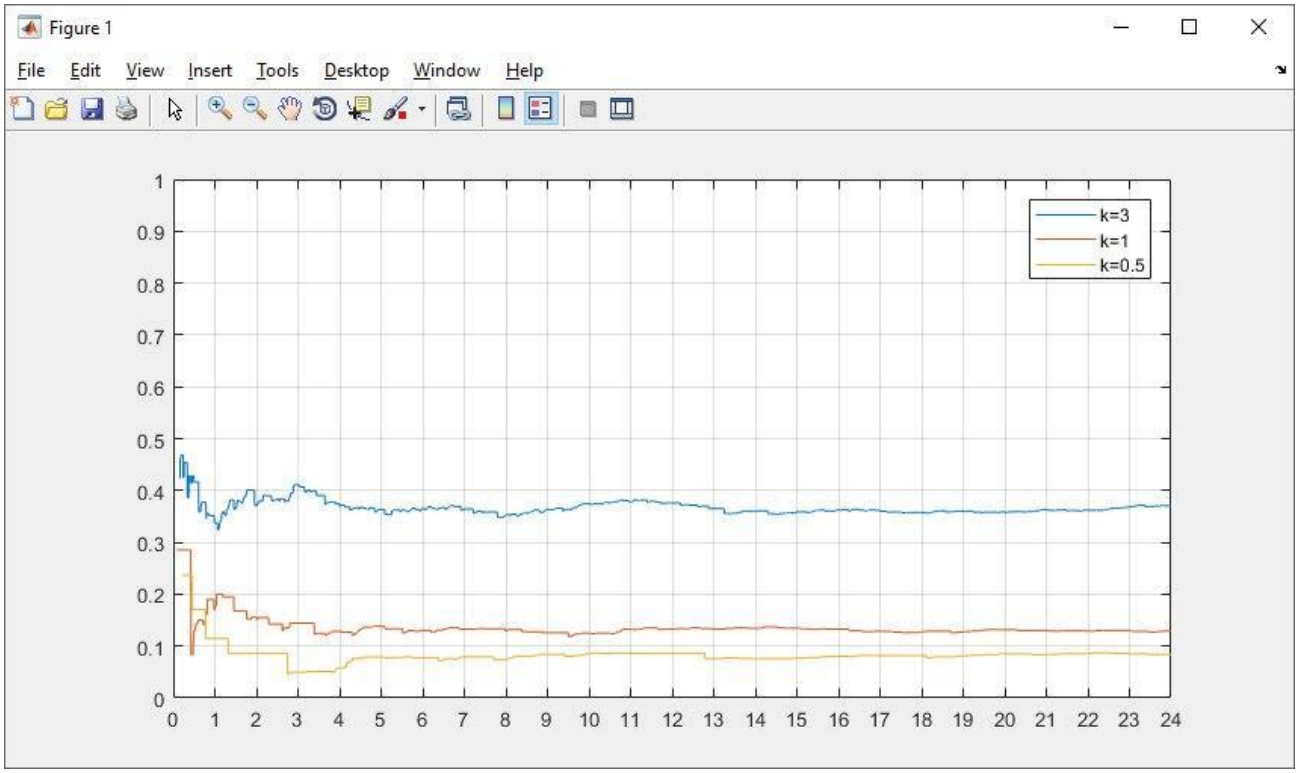


Рисунок В.4– Вплив на систему джерела негативного впливу 4ї кваліфікації

На рисунках В.5-В.8 представлено вірогідність надійності інформаційної системи при конфлікті з одним джерелом негативного впливу та наявним засобом захисту інформації.

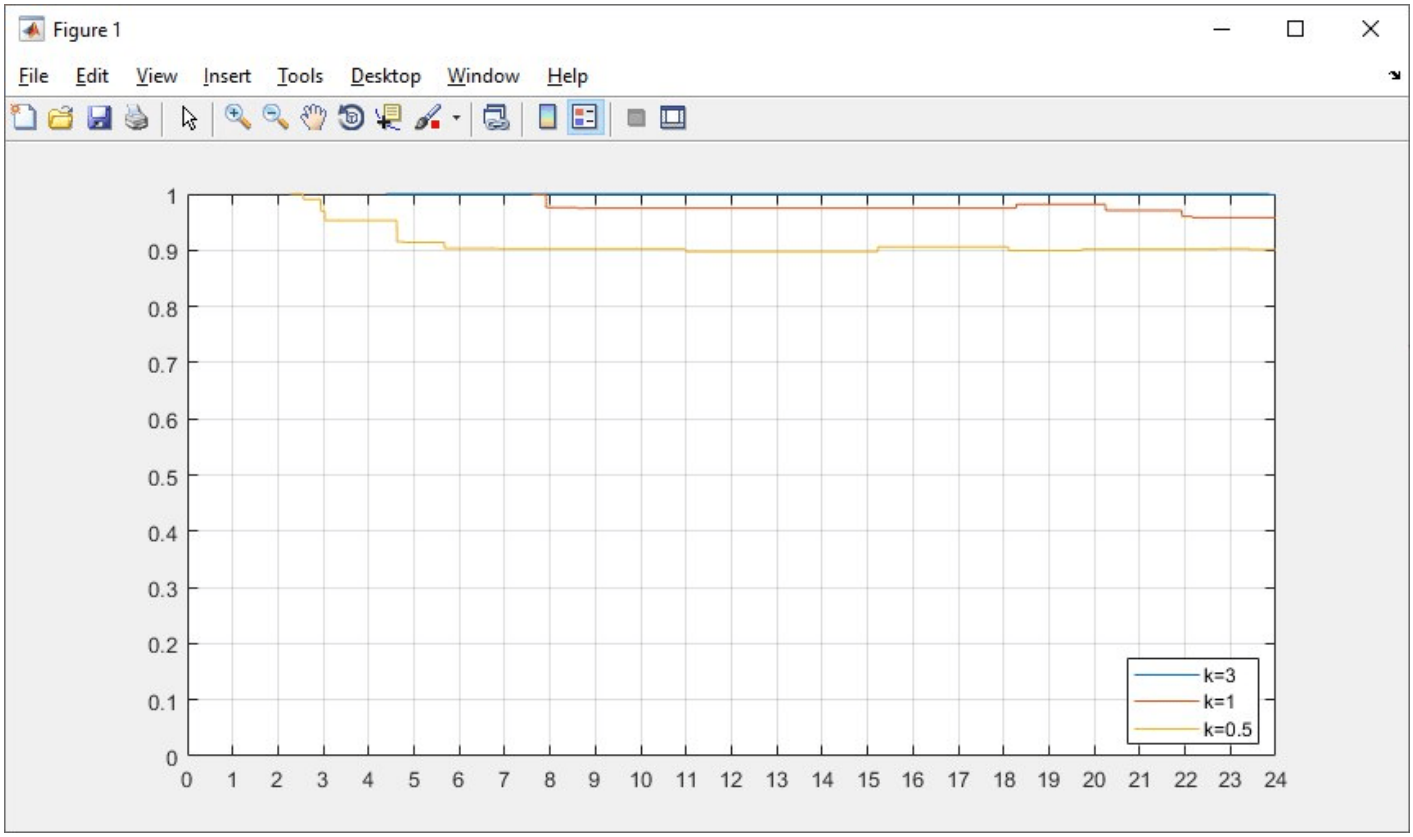


Рисунок В.5 – Вплив на систему джерела негативного впливу 1ї кваліфікації

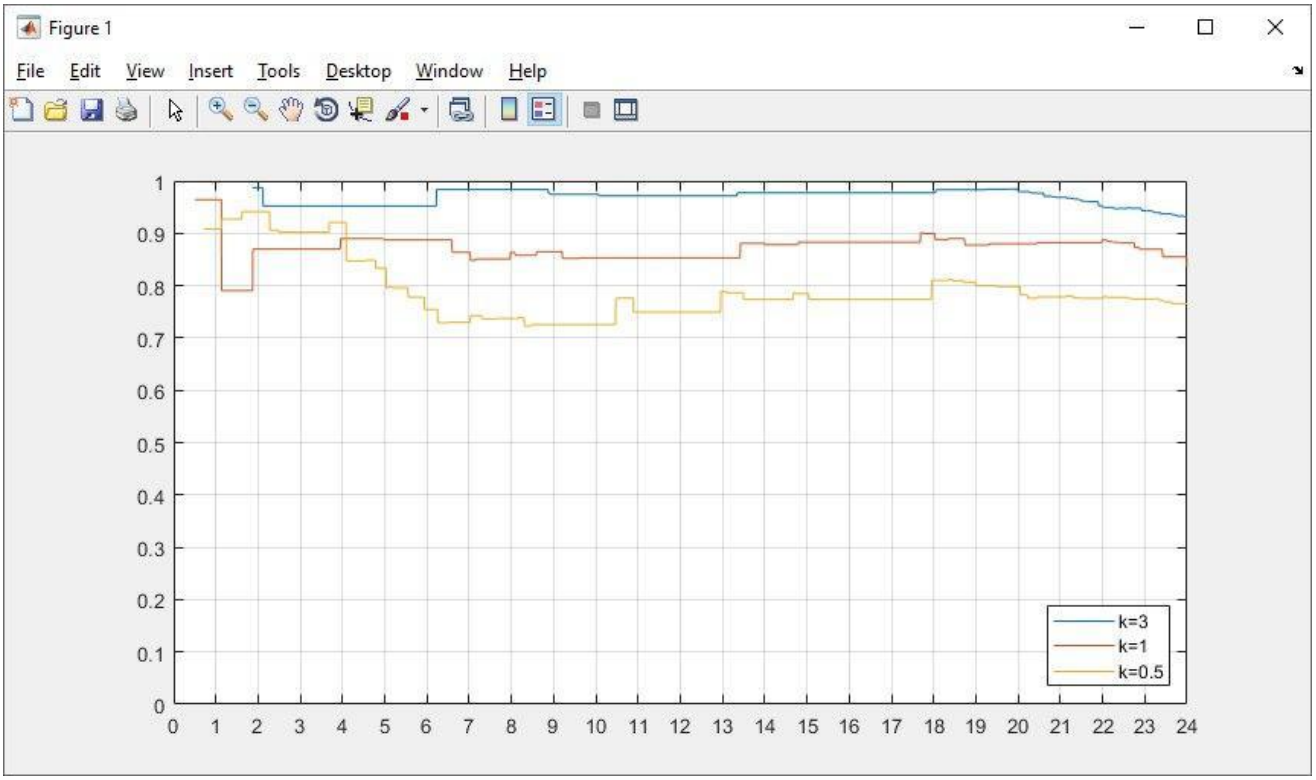


Рисунок В.6 – Вплив на систему джерела негативного впливу 2ї кваліфікації

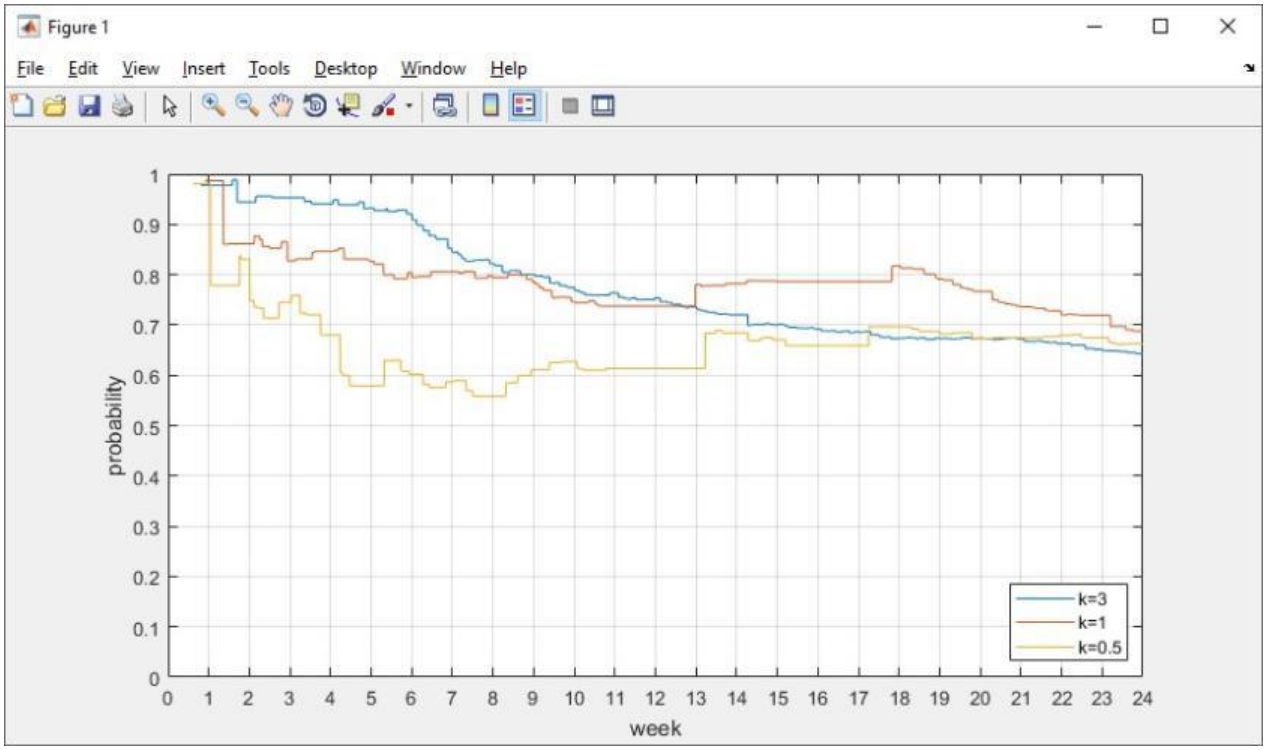


Рисунок В.7 – Вплив на систему джерела негативного впливу 1ї кваліфікації

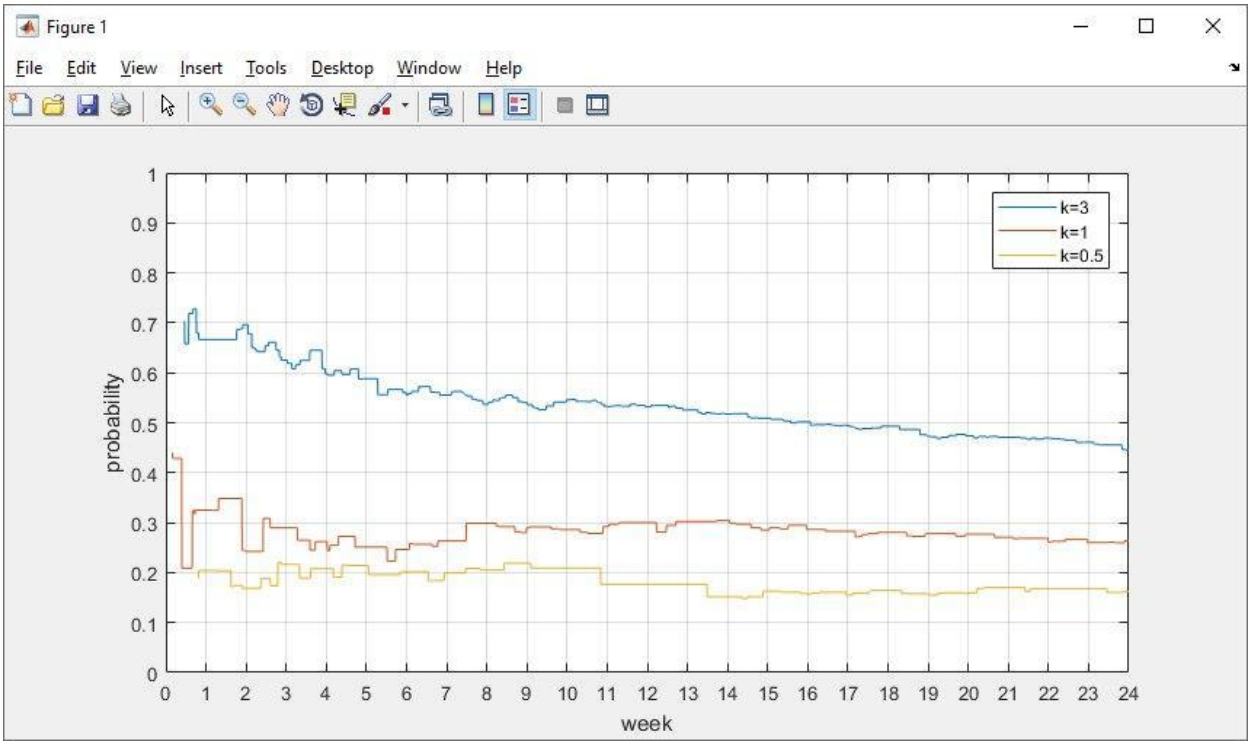


Рисунок В.8 – Вплив на систему джерела негативного впливу 1ї кваліфікації

На рисунках В.9-В.12 представлено вірогідність надійності інформаційної системи при конфлікті з коаліцією джерел негативного впливу

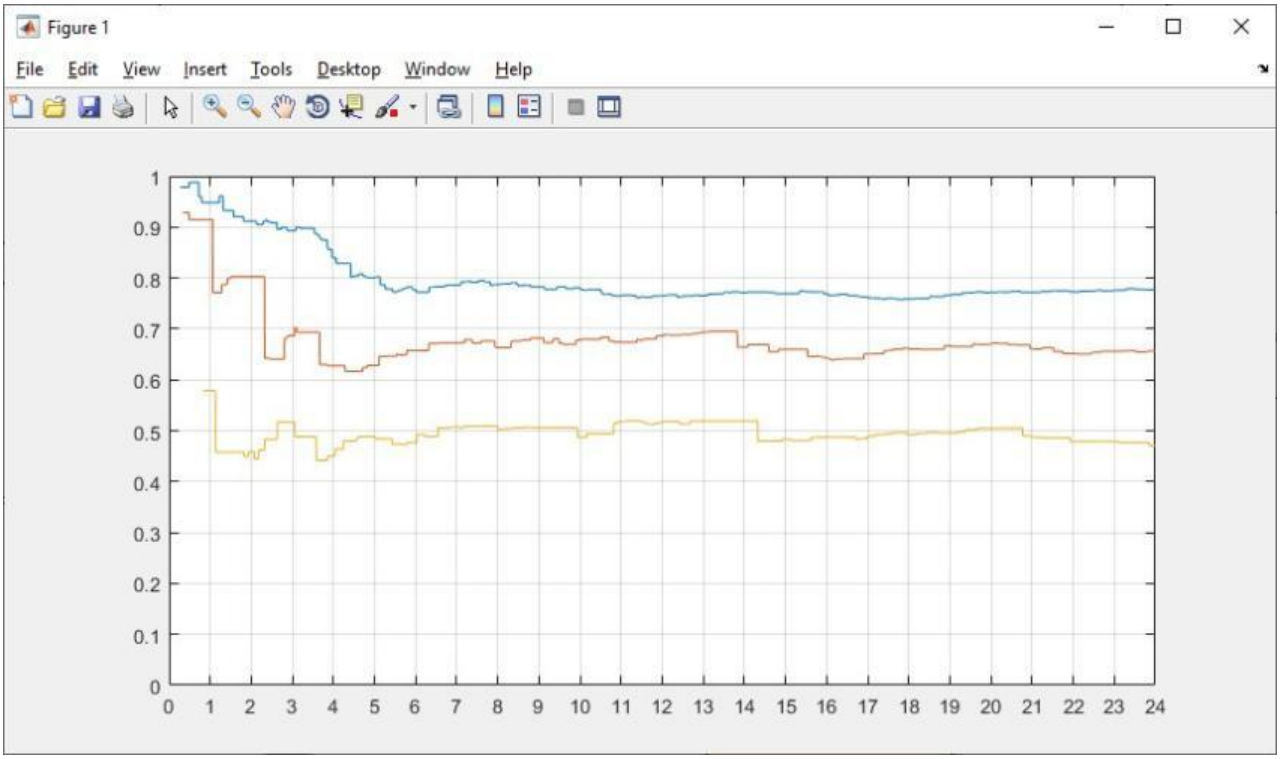


Рисунок В.9 – Вплив на систему джерела негативного впливу 1ї кваліфікації

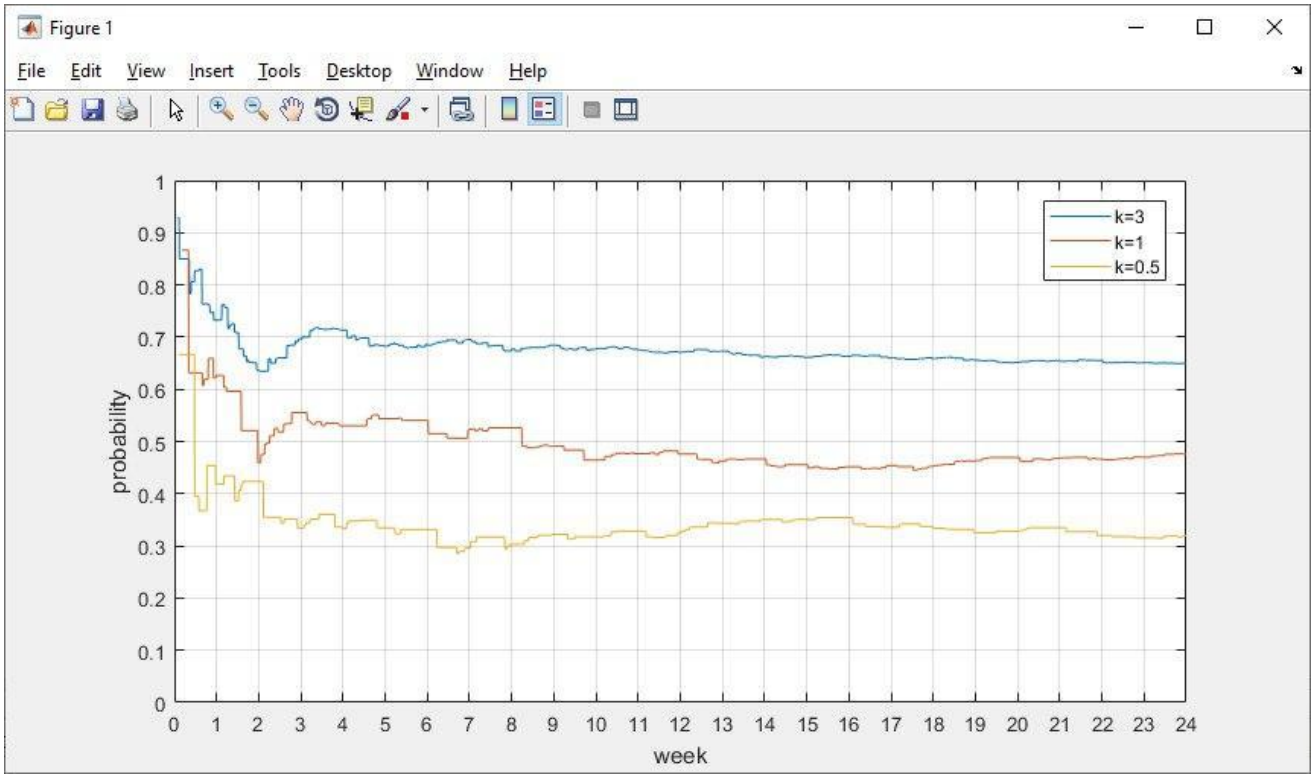


Рисунок В.10 – Вплив на систему джерела негативного впливу 2ї кваліфікації

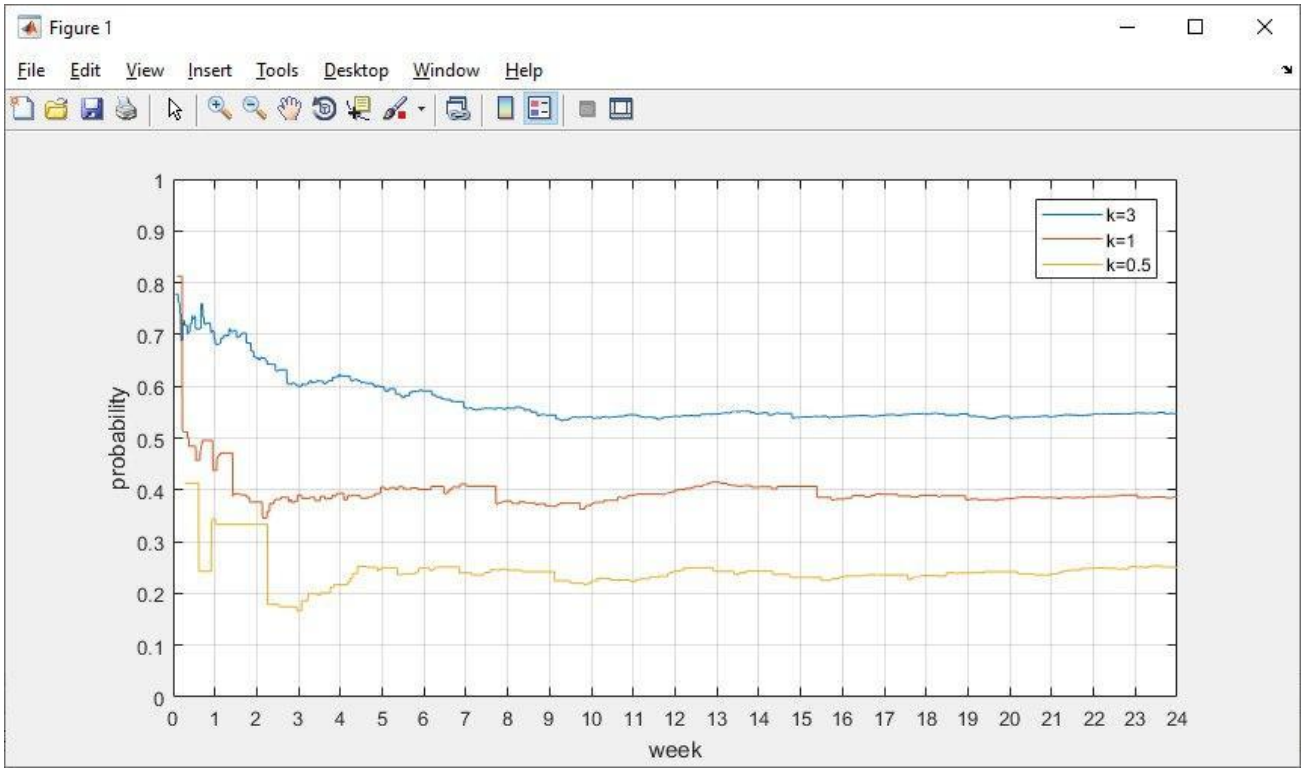


Рисунок В.11 – Вплив на систему джерела негативного впливу 3ї кваліфікації

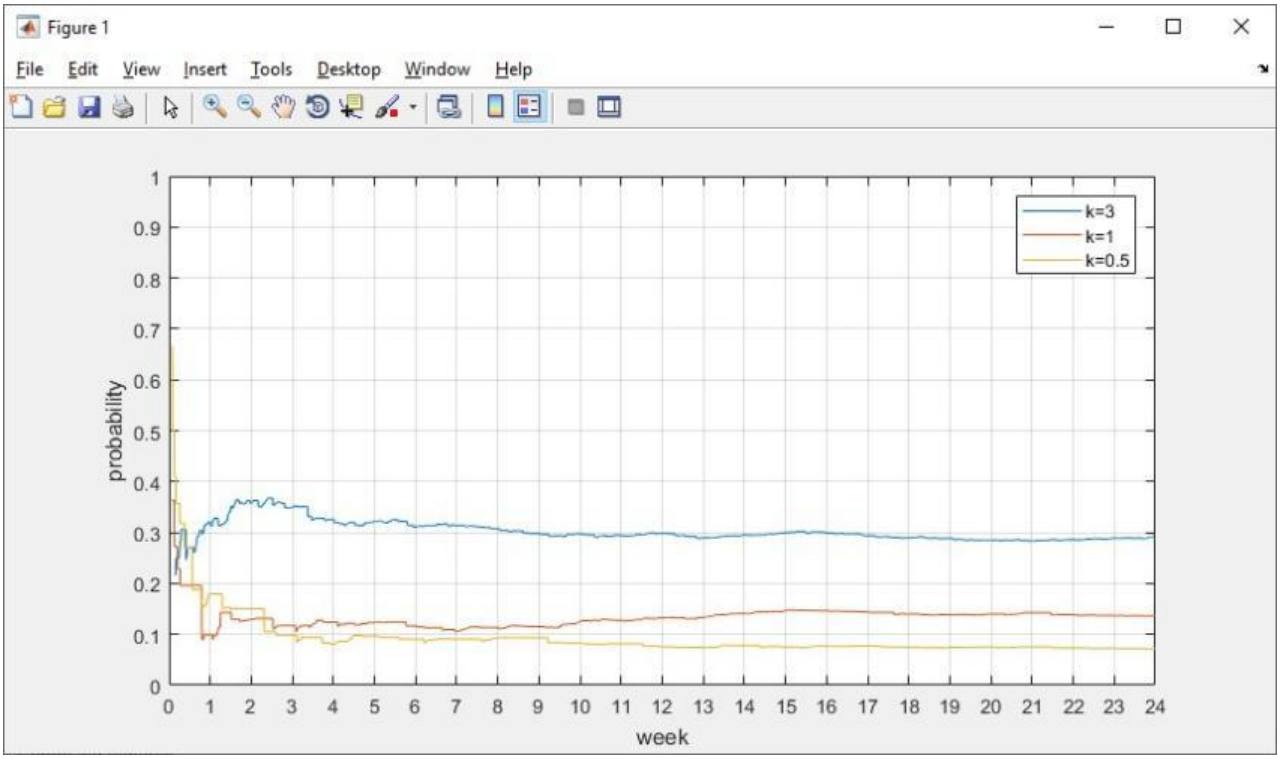


Рисунок В.12 – Вплив на систему джерела негативного впливу 4ї кваліфікації

На рисунках В.13-В.16 представлено вірогідність надійності інформаційної системи при конфлікті з коаліцією джерел негативного впливу та інсайдером в системі.

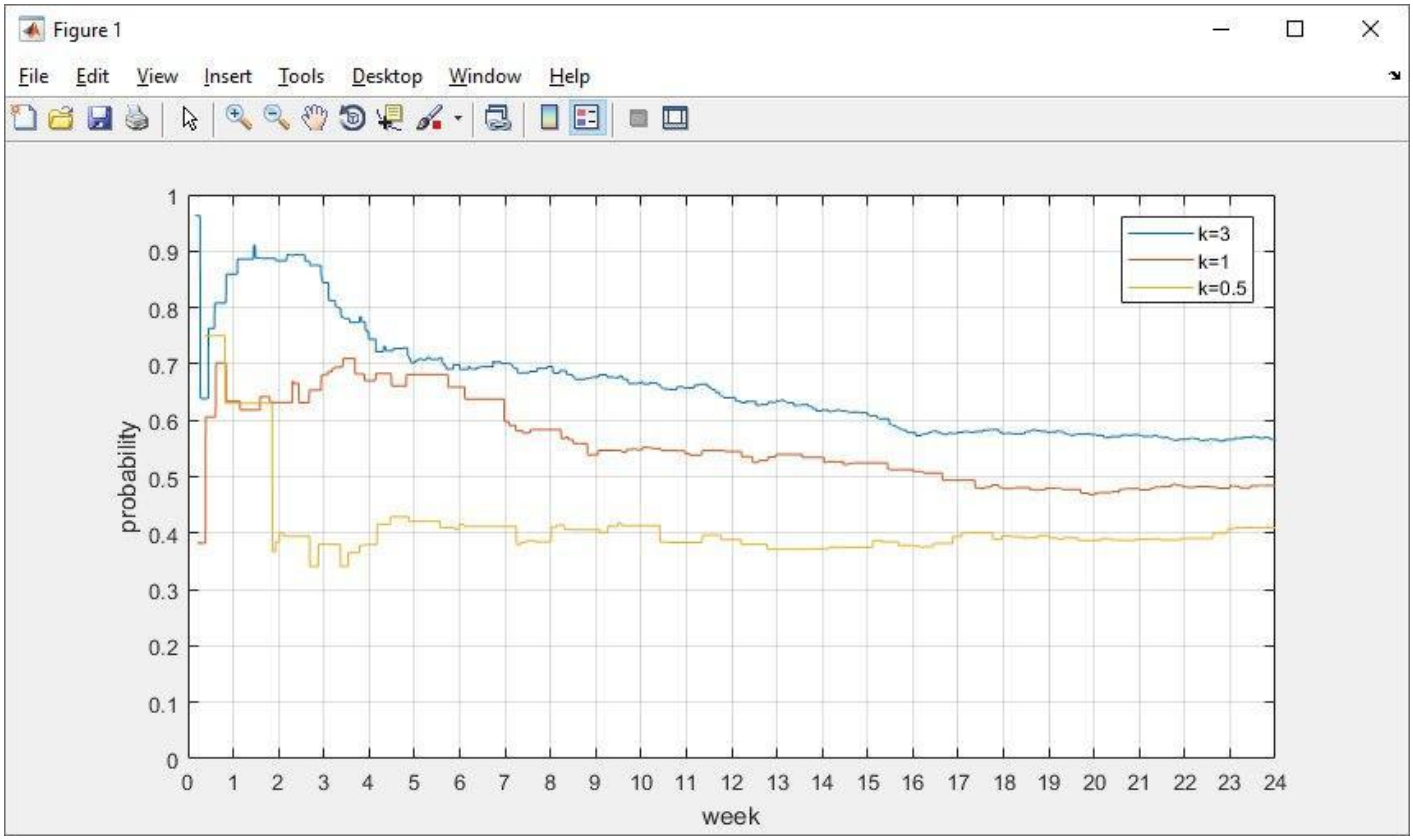


Рисунок В.13 – Вплив на систему джерела негативного впливу 1ї кваліфікації

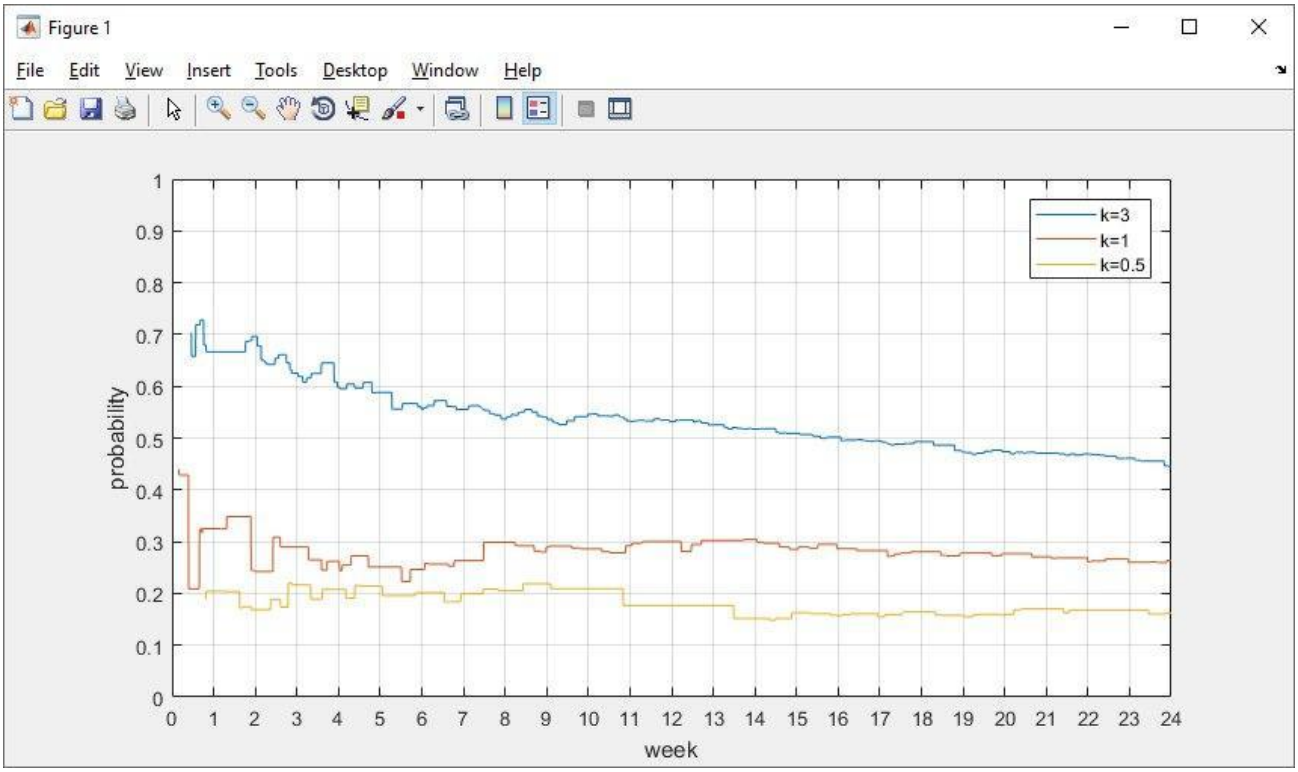


Рисунок В.14 – Вплив на систему джерела негативного впливу 2ї кваліфікації

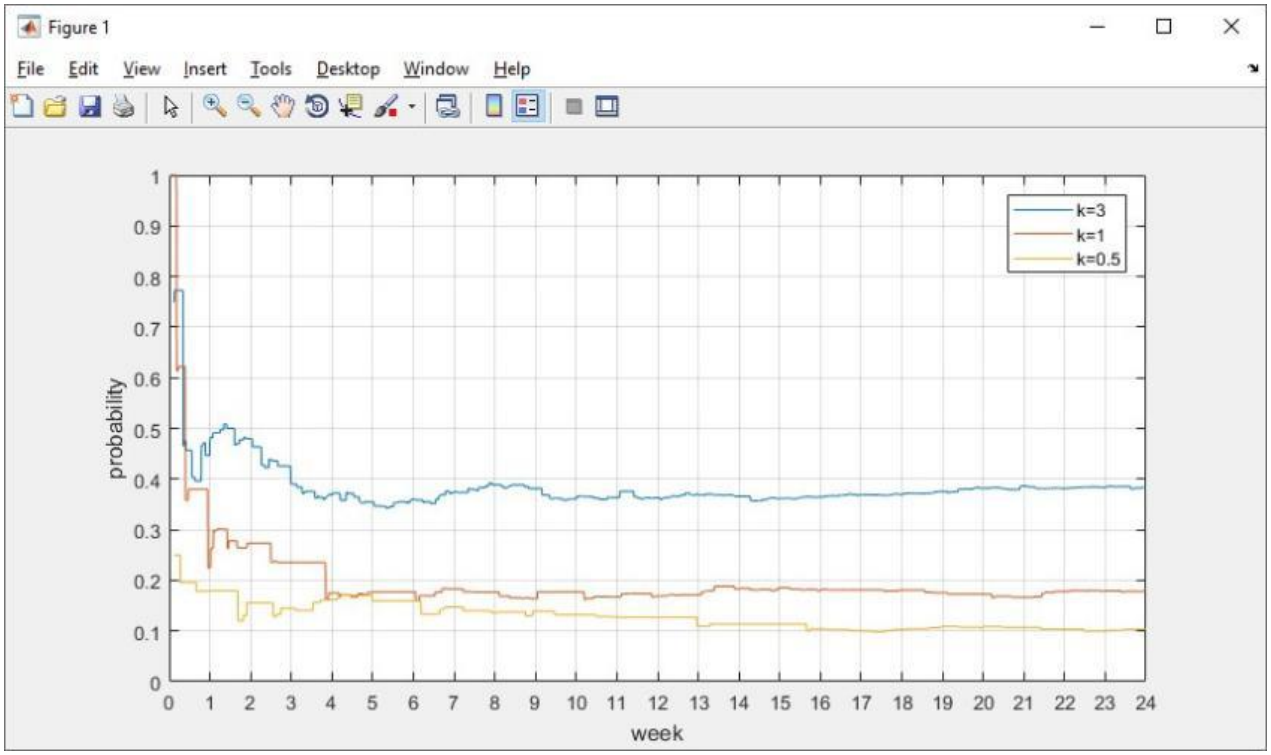


Рисунок В.15 – Вплив на систему джерела негативного впливу 3ї кваліфікації

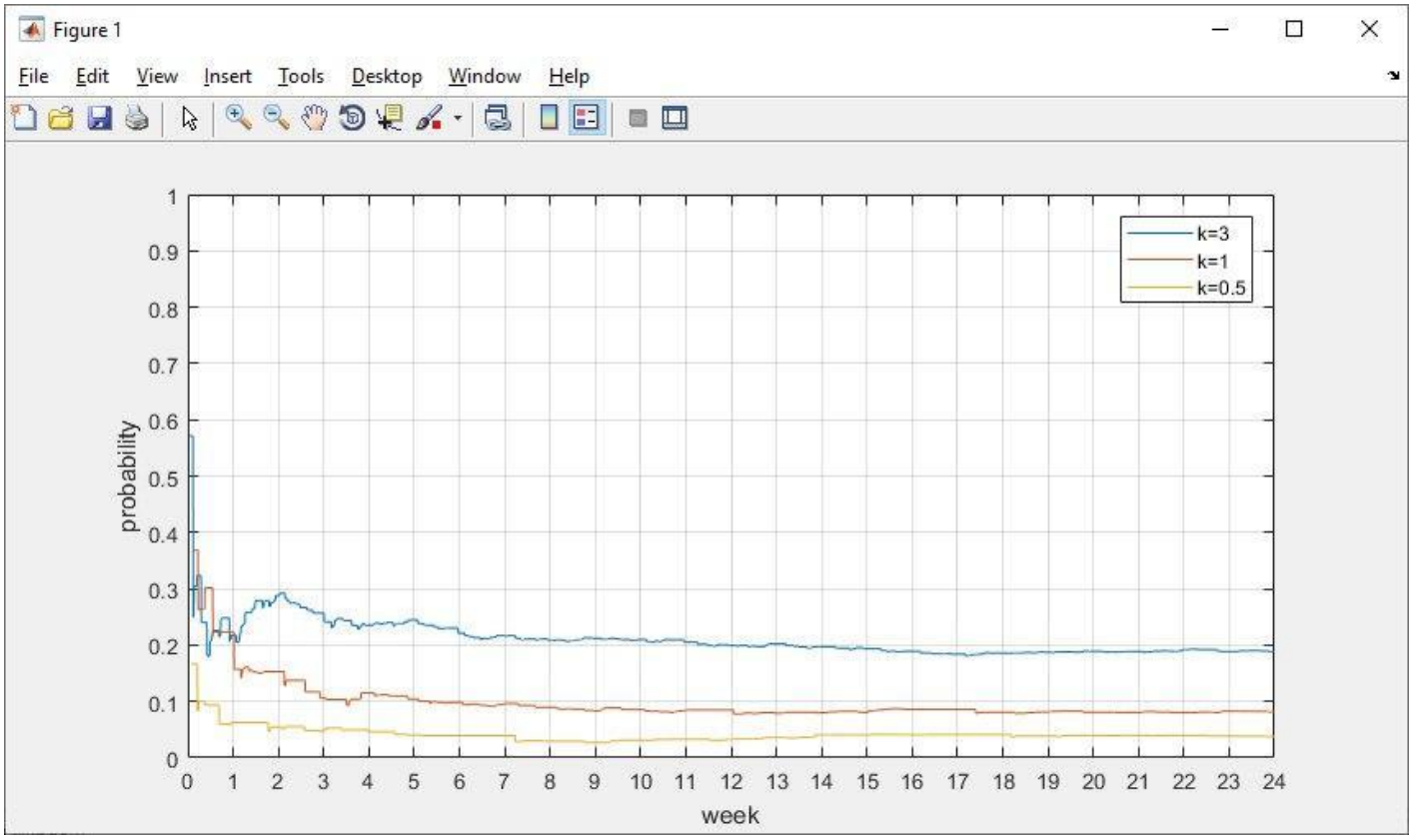


Рисунок В.16 – Вплив на систему джерела негативного впливу 4ї кваліфікації

Був наведений лише кілька прикладів відносно кваліфікації адміністратора.
Як варіант, нижче на рисунках В.17-В.18 представлено графіки надійності системи при кваліфікаціях адміністратора 3 та впливах різної кваліфікації.

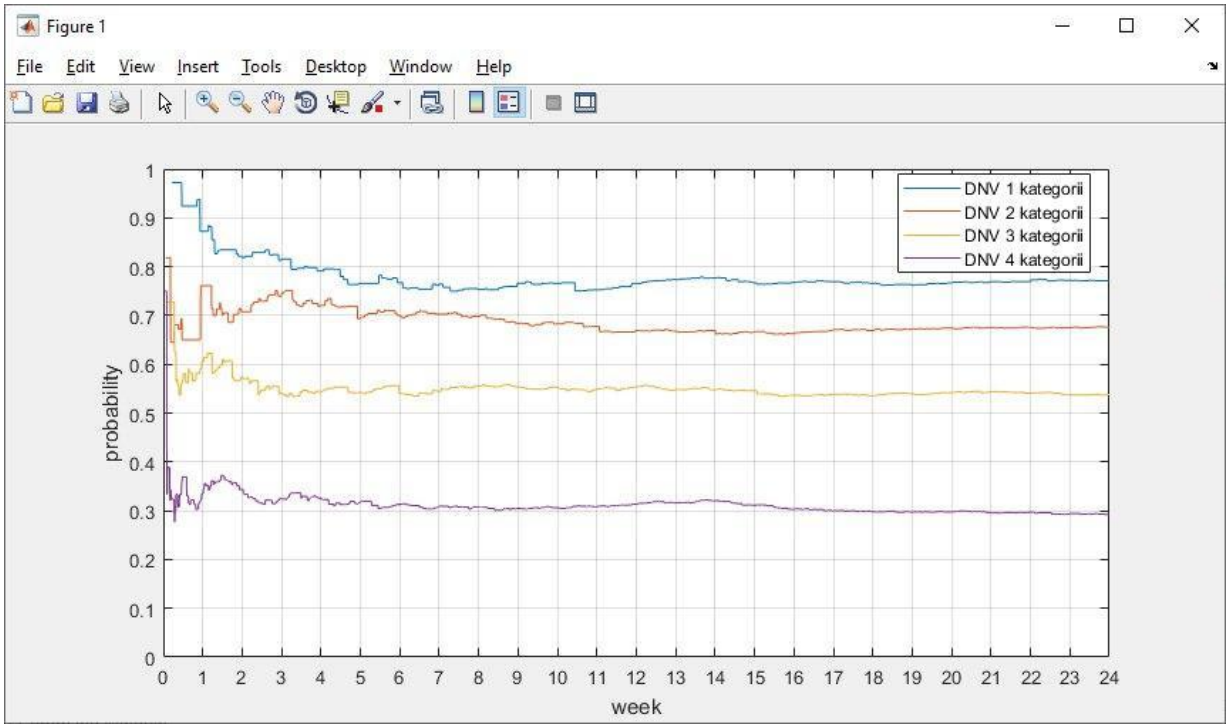


Рисунок В.17 – Вплив на систему при коаліції джерел негативного впливу при k=3

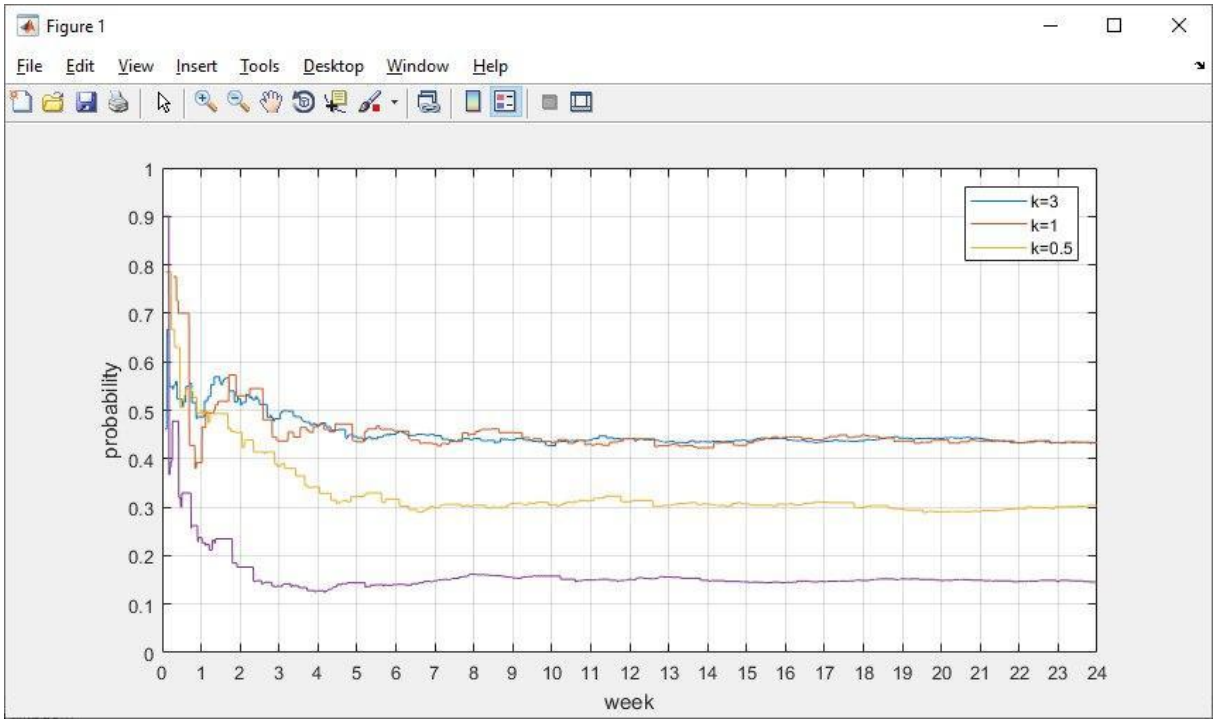


Рисунок В.18 – Вплив на систему при коаліції джерел впливу з інсайдером при k=3

ДОДАТОК Г АКТ ВПРОВАДЖЕННЯ

Затверджую
Перший проректор
Сумського державного університету

_____Карпуша В.Д.

«_____»_____2020р.

АКТ
Впровадження в навчальний процес
СУМСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ
результатів наукової роботи
студентки групи ІТ.м – 91 Сумського державного університета
Щербань Тетяни Володимирівни
на тему
«Інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів»

Складений 1 грудня 2020 р. комісією у складі:

Голова комісії:

Доцент кафедри комп'ютерних наук, зав. секції «Інформаційні технології проектування», кандидат технічних наук, доцент ***Шендрик В.В.***

Члени комісії:

1. *Професор кафедри комп'ютерних наук, доктор технічних наук, професор* ***Лавров Є.А.***
2. *Доцент кафедри комп'ютерних наук, кандидат технічних наук, доцент* ***Чибіряк Я.І.***
3. *Аспірант кафедри комп'ютерних наук,* ***Данілова Л.В.***

В період з *1 грудня 2020 р. по 10 грудня 2020 р.* комісія провела роботу з визначення впровадження результатів Щербань Т.В. в навчальний процес кафедри комп'ютерних наук.

Результати роботи комісії

1. На кафедру комп'ютерних наук передано комплекс програм «Інформаційна технологія аналізу ймовірнісних характеристик надійності використання програмного забезпечення інформаційної системи в умовах навмисних негативних впливів».
2. Матеріали використані в дисципліні **«Теорія ризиків»** для студентів бакалавратури, що навчаються за освітньою програмою «Кібербезпека» в наступних лабораторних роботах:
   - прийняття рішень у кібербезпеці за умов ризику (4 години);
   - практичне застосування методів імітаційного моделювання в задачах управління ризиками. Simulink технологія моделювання ризиків (4 години);
   - практичне застосування методів імітаційного моделювання в задачах управління ризиками. Stateflow моделі управління ризиками (4 години).

Використання результатів дипломної роботи у навчальному процесі Сумського державного університету дозволяє підвищити якість підготовки фахівців.

Голова комісії _____ Шендрик В.В.
Члени комісії _____ Лавров С.А.
_____ Чибіряк Я.І.
_____ Данілова Л.В.

ДОДАТОК Ґ ПУБЛІКАЦІЇ

Аналіз проблем людського фактору в задачах забезпечення кібербезпеки

Кіншаков Е., Щербань Т.
Науковий керівник – професор Лавров Е.А.
Сумський державний університет, Суми, Україна

Проблеми кібербезпеки набули надзвичайної актуальності.Інформаційна безпека (ІБ) складається з цілого комплексу різних заходів і дій. Це, перш за все, контроль дій різного роду суб'єктів - рядових співробітників компанії, привілейованих користувачів, IT-аутсорсерів, контрагентів. Крім того, це чітке розмежування прав доступу всередині компанії, використання резервного копіювання даних, а також наявність простої, зрозумілої і доведеної до відома працівників політики безпеки. У поточних реаліях захист повинен бути досить гнучким, щоб забезпечити і достатній рівень захищеності, і виконання бізнес-цілей. Згідно з інформацією, яка міститься в дослідженні Lloyd's of London і Cyence, фінансові втрати від масштабної кібератаки можуть коштувати світовій економіці від 15,6 млрд до 121 млрд доларів. Якщо розглядати найбільш песимістичний сценарій розвитку подій, то втрати від кібератак можуть перевищити економічний збиток від урагану «Катріна», який став найбільш руйнівним в історії Сполучених Штатів. Втрати від нього склали 108 млрд доларів. У доповіді вказуються два потенційних сценарію розвитку глобальної кібератаки: злом провайдерів хмарних сховищ або використання можливих вразливостей в операційних системах.

У першому сценарії хакери модифікують «гіпервизор», керуючу систему хмарних сховищ, в результаті чого всі зберігаються файли виявляються загубленими. У другому варіанті розглядається гіпотетичний випадок, коли кібераналітік випадково забуває в поїзді сумку, в якій зберігається доповідь про уразливість всіх версій операційної системи, встановленої на 45% всіх світових пристроїв. Ця доповідь згодом продається кримінальним групам. Мінімальний збиток при першому сценарії складе від 4,6 млрд до 53,1 млрд доларів. При другому сценарії втрати складуть від 9,7 млрд до 28,7 млрд доларів.

Людський фактор. Саме проблема «надійних рук» або, кажучи іншими словами, кваліфікованих кадрів є однією з найбільш нагальних. Вона має особливу актуальність протягом усіх останніх років, тому що на сьогоднішній день людина залишається найбільш уразливим ланкою в IT-інфраструктурі.Найслабша ланка в інформаційній безпеці банку - це співробітник компанії. Якщо співробітники не дотримуються правил безпеки, то технології не зможуть допомогти захиститися.

Так, при використанні соціальної інженерії зловмисники можуть змусити співробітника організації здійснити якусь дію, яке спростить проведення атаки, пояснює експерт. «Часто, щоб підібрати пароль до аккаунту, зловмиснику не обов'язково його« зламувати »- вся інформація про

пароль є в профілі соціальних мереж або поруч з робочим столом. Навіть співробітники на керівних позиціях виробляють маніпуляції, спровоковані зловмисниками. Окремим рядком можна привести небажання працівників слідувати політиці і вимогам по ІБ заради спрощення своєї роботи». Щоб мінімізувати вплив людського фактора, потрібно постійно підвищувати обізнаність співробітників в області ІБ, а також впроваджувати систему контролів і моніторингу дотримання політик і вимог в області ІБ. Серед основних способів мінімізації загрози ІБ -підвищення обізнаності персоналу в питаннях ІБ, проведення тестів, ділових ігор, кібернавчань.

У зв'язку з проблемою ризиків, які несе людський фактор, цікаво згадати дослідження антивірусної компанії ESET, опубліковане в липні 2017 року. Чотири компанії з п'яти недооцінюють ризики ІБ, пов'язані з людським фактором. Такий висновок зробили співробітники ESET після опитування інтернет-користувачів з СНД. Респондентам запропонували вибрати відповідь на питання «Чи проходили ви на роботі тренінг з інформаційної безпеки?». Негативна відповідь лідирує з великим відривом. 69% респондентів ніколи не проходили навчання основам кібербезпеки в своїх компаніях. Ще 15% учасників опитування повідомили, що їх роботодавці обмежилися мінімальним обсягом інформації. Навчання не виходило за рамки «в разі неполадок перезавантажте комп'ютер», правила кібербезпеки не зачіпалися. Тільки 16% респондентів пройшли якісні тренінги з докладною розповіддю про інформаційну безпеку. Для порівняння: більше 60% учасників аналогічного опитування в США повідомили, що їх роботодавці організували для них навчання з кібербезпеки.

Аналіз основних визначень і підходів до організації обробки персональних даних

Ковальчук Я.В.
Науковий керівник – к.т.н., доц. Джулій В.М.
Хмельницький національний університет

Інформація, яка містить відомості про фізичних осіб (громадян) - персональні дані, використовуються в різних системах обробки інформації все частіше, що обумовлено постійним розширенням сфери застосування інформаційних технологій для обслуговування населення. Специфіка роботи з персональними даними заснована на потенційній можливості їх використання для заподіяння шкоди суб'єктам, до яких відносяться дані - власникам персональних даних. Особлива увага приділяється питанням захисту персональних даних (ПД) в автоматизованих інформаційних системах ПД – (ІСПД). Вимоги до захисту в ІСПД, відповідно до низки документів, враховують категорію і кількість ПД, специфіку вирішуваних завдань і ряд інших показників. Виконання цих вимог, як правило, пов'язане з

Министерство образования и науки РФ ■ Петрозаводский государственный университет ■ Московский международный университет ■ ООО «ФОРС – Центр разработки» ■ ООО «Интернет-бизнес-системы» ■ Институт прикладных математических исследований КарНЦ РАН

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ, НАУКЕ, ОБЩЕСТВЕ

Материалы XII всероссийской
научно-практической конференции

(4–6 декабря 2018 года)

Петрозаводск
2018

МОДЕЛИ ДЛЯ ЭРГОНОМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРОВ, УПРАВЛЯЮЩИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Е. А. Лавров, Т. В. Щербань, Ю. С. Михайленко, А. В. Федорова
Сумский государственный университет
Сумы
prof_lavrov@mail.ru

Рассмотрены проблемы создания систем информационной безопасности автоматизированных систем. Обоснована необходимость эргономического обеспечения деятельности операторов. Разработана структура системы эргономического обеспечения операторов, описаны основные задачи и подходы к их решению.

Ключевые слова: эргономика, кибербезопасность, информационная безопасность, управление инцидентами, надежность, человек-оператор, система управления.

MODELS FOR ERGONOMIC MAINTENANCE OF OPERATORS MANAGING INFORMATION SECURITY OF COMPLEX AUTOMATED SYSTEMS

E. A. Lavrov, N. B. Pasko, T. V. Shcherban, Y. S. Mikhaylenko, A. V. Fedorova
Sumy state university
Sumy

The problems of creating information security systems of automated systems are considered. The necessity of ergonomic support for the activities of operators has been substantiated. The structure of the system of ergonomic support of operators was developed, the main tasks and approaches to their solution were described

Key words: ergonomics, cybersecurity, information security, incident management, reliability, human operator, control system.

Исходные предпосылки. Создание системы управления информационной безопасностью (обозначаются аббревиатурой SIM (Security Information Management), SIEM (Security Information and Event Management), Cyber Security and Management (CSM)) предполагает создание системы поддержки принятия решений, направленных на минимизацию последствий различных нарушений, в т. ч. инцидентов безопасности. Известно мнение, что инцидент — любое событие, которое не является частью стандартного функционирования, которое приводит или может привести к остановке или снижению качества функционирования или предоставления услуги [1].

Проблемы управление инцидентами и постановка задач исследования. Главная цель процесса управления инцидентами — восстановить штатное функционирование и минимизировать отрицательное влияние инцидентов на бизнес-процессы [1]. Основные действия, выполняемые в процессе управления инцидентами (Рис. 1).

- обнаружение и регистрация инцидента;
- классификация и первичная поддержка;

- расследование и диагностика;
- разрешение и восстановление;
- закрытие инцидента.

Качество работ по управлению инцидентами существенно зависит от характеристик и организации деятельности операторов, задействованных в процессе реализации этих этапов:

- квалификация,
- мотивация,
- функциональное состояние,
- загруженность,
- операционно-типовая напряженность деятельности,
- условия труда на рабочем месте,
- качество информационной модели,
- степень автоматизации,
- наличие процедур поддержки принятия решений,
- распределение функций между операторами,
- др.

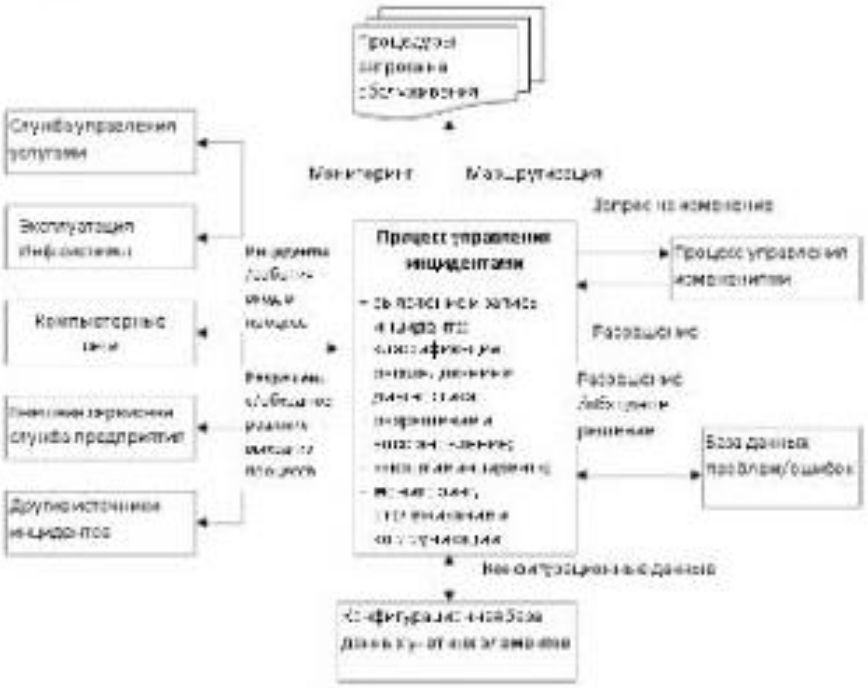


Рис. 1 Схема процесса управления инцидентами

Целью настоящей работы является разработка структуры системы эргономического обеспечения деятельности операторов управляющих информационной безопасностью сложных автоматизированных систем.

Разработка номенклатуры задач эргономического обеспечения системы управления информационной безопасностью. Основными задачами эргономики в информационной безопасности должны быть:

- определение численности операторов и их квалификации,
- определение степени автоматизации расследования и устранения инцидентов (распределение функций между операторами и средствами автоматики),
- распределение функций между операторами и проектирование групповой деятельности по расследованию и устранению инцидентов,
- проектирование условий труда (в т. ч. по темпу и количеству обрабатываемых заявок),
- проектирование информационных моделей адаптивных интерфейсов для операторов,
- проектирование алгоритмов деятельности по расследованию и устранению инцидентов операторов.

Принципы разработки информационных моделей для операторов. При автоматизации процессов управления инцидентами необходимо уделять внимание автоматизированной обработке событий информационной безопасности —основе практически любого инцидента. События от различных технических средств защиты являются важнейшим поставщиком информации о процессах, происходящих в системе управления информационной безопасностью, нарушениях, рисках. На основании событий проводятся корректирующие действия, оценка текущей защищенности системы, эффективности функционирования системы информационной безопасности. Только обладая полными и достоверными наборами событий, можно провести надлежащее расследование инцидентов. События — основной канал обратной связи для управляющих воздействий в рамках системы управления информационной безопасности. Если соответствующая база данных отсутствует, информация об имеющих отношение к инциденту единицах конфигурации будет добываться вручную, что существенно увеличит время обработки инцидента и повысит ее сложность. Для поддержания процесса обработки событий на уровне, обеспечивающем информационное обеспечение операторов технической поддержки, необходима автоматизированная система управления обработкой событий (АСУОС).

АСУОС должна:

- собирать события от всех информационно-технических средств и возможных источников инцидентов;
- приводить события к единому формату;
- осуществлять хранение событий;
- формировать информационные модели операторов системы и отчетные формы в режиме OLAP.

Собранные данные должны подвергаться корреляции и формировать информационную модель (специальный интерфейс) операторов.

Средства поиска, предоставляемые оператору, должны позволяют осуществлять оперативное и всестороннее расследование инцидентов.

Модели для СППР деятельности оператора в системе управления информационной безопасностью. Управление инцидентами являются достаточно сложным процессом при реализации всех процедур. Поэтому при внедрении описанного процесса, как правило, прибегают к средствам

автоматизации. Однако, представленные на рынке программных продуктов системы не в полной мере решают проблему информационной поддержки принятия решений операторов-руководителем. Известные программы не позволяют оператору-руководителю в условиях информационной напряженности и дефицита времени оценить последствия распределения работ и выбрать оптимальный вариант.

Основными проблемами являются:

- Какими операторам поручить работы по устранению нарушений?
- Как диагностировать причины нарушения?

В связи с этим нами разрабатываются элементы СППР, позволяющие:

- оценить вероятность безошибочного реализации алгоритмов деятельности по устранению нарушений конкретными операторами и таким образом предложить оптимальную технологию решения задачи;
- документировать возникающие дефекты с указанием возможных причин их возникновения (База данных «Проблемы (ошибки)»);
- на основе анализа информации, накопленной в Базе данных «Проблемы» с использованием моделей DATA MINING (нейронная сеть, fuzzy logic, деревья решений, байесовские модели и др.) оценивать возможные источники и причины нарушений.

Для задач проектирования и оптимизации деятельности используется методология функционально-структурной теории эргатических систем профессора Губинского А.И. [2], модели и программные средства [3–6].

Библиографический список:

2. https://www.osp.ru/os/2001/07-08/180310/
3. Информационно-управляющие человеко-машинные системы: исследование, проектирование, испытания: Справочник/Под общ. ред. А. И. Губинского и В. Г. Евграфова. -М.: Машиностроение, 1993. -528с.
4. Lavrov, E. Mathematical models for the distribution of functions between the operators of the computer-integratedflexible manufacturing systems/N. Pasko, A. Krivodub, A. Tolbatov//Proceedings of the XIII-th international conference tcset'2016 «Modern problems of radio engineering, telecommunications, and computer science». -Lviv-Slavsko, Ukraine, february 23 -26, 2016. -p. 72–76.
5. Лавров Е.А., Пасько Н.Б., Федорова А.В., Плеканов Е. Диалоговый моделирующий квалиметрический комплекс для эргономического обеспечения цифровых технологий управления // В сборнике: Цифровые технологии в образовании, науке, обществе Материалы XI (1) всероссийской научно-практической конференции, Петрозаводск, 27—30 ноября 2017 г. — Петрозаводск, 2017. — С. 87–90.
6. Лавров Е.А., Пасько Н.Б., Щербань Т.В., Михайленко Ю. С. Совершенствование цифровых технологий производства методами оптимального управления человеко-машинными взаимодействиями// В сборнике: Цифровые технологии в образовании, науке, обществе Материалы XI (1) всероссийской научно-практической конференции, Петрозаводск, 27—30 ноября 2017 г.- Петрозаводск, 2017.- С. 90–94.


МАТЕРИАЛЫ КОНФЕРЕНЦИИ
№ (1) Всероссийская научно-практическая конференция
ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ, НАУКЕ, ОБЩЕСТВЕ
МАТЕРИАЛЫ КОНФЕРЕНЦИИ
Петрозаводск, 27–30 ноября, 2017
11/001
ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ, НАУКЕ, ОБЩЕСТВЕ 11/001
11/001

proceedings of the IV international scientific conference, May 25-27, 2016 - Sumy: Sumy State University, 2016. - P. 89.

12. Lavrov, E. Information technology for distribution of functions between operators in automated systems. Analysis of efficiency. [Text] / E. Lavrov, N. Pasko, // International Scientific Conference «UNITECH '15». Proceedings. 18-19 November 2015, Gabrovo, Bulgaria. - Gabrovo: University Publishing House «V.APRILOV», 2015. – Volume 2. - P.p 298-306.
13. Lavrov E. Development of models for the formalized description of modular e-learning systems for the problems on providing ergonomic quality of human-computer interaction/ E Lavrov, N Barchenko, N Pasko, I Borozenec// Eastern-European Journal of Enterprise Technologies 2 (2 (86)), 4–13.
14. Bahmach M., Lavrov E. Program Complex of Statistical Calculations for Control the Quality of Products at Lebedinsky Plant of Piston Rings Advanced Information Systems and Technologies: proceedings of the IV international scientific conference, May 25-27, 2016– Sumy: Sumy State University, 2016. – P. 82-84.
15. Бахмач Н.В., Лавров Е.А. Формализованное описание производственных процессов на Лебединском заводе поршневых колец для задач управления качеством // Інформатика, математика, автоматика: матеріали та програма науково-технічної конференції, м. Суми, 18-22 квітня 2016 р. – Суми : СумДУ, 2016. – С. 90.
16. 16.Лавров Е.А., СкиданенкоА.С. Эргономические резервы повышения эффективности АСУТП производства удобрений //Сучасні інформаційні системи і технології: Матеріали Другої міжнародної науково-практичної конференції, м. Суми, 21-24 травня 2013 р.— Суми : СумДУ, 2013. — С. 53-54.

СОВЕРШЕНСТВОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРОИЗВОДСТВА МЕТОДАМИ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ ЧЕЛОВЕКО-МАШИННЫМ ВЗАИМОДЕЙСТВИЕМ

Е. А. Лавров, Н. Б. Пасько, Т. В. Щербань, Ю. С. Михайленко
Сумский государственный университет
Сумы
prof_lavrov@mail.ru

Проанализированы эргономические проблемы современного цифрового управления. Предложен метод оптимизации алгоритма деятельности человека-оператора. Охарактеризована сфера возможных применений метода. Предложены пути широкого внедрения методов оптимизации в практику эргономического обеспечения.

Ключевые слова: цифровая технология производства, эргономика, человек-оператор, деятельность, оптимизация, надежность.

IMPROVEMENT OF DIGITAL TECHNOLOGIES OF PRODUCTION BY METHODS OF OPTIMUM CONTROL OF HUMAN-MACHINE INTERACTION

E. A. Lavrov, N. B. Pasko, T. V. Shcherban, Y. S. Milchaylenko
Sumy State University
Sumy

Ergonomic problems of modern digital control are analyzed. A method for optimizing the algorithm of human operator activity is proposed. The sphere of possible applications of the method is characterized. Ways of wide introduction of optimization methods in the practice of ergonomic provision are suggested.

Key words: digital production technology, ergonomics, human operator, activity, optimization, reliability.

Введение. Последние годы охарактеризованы быстрым изменением характера автоматизированного управления технологиями [1-3]:

- получили широкое распространение цифровые распределенные системы информационные системы
- увеличилось количество операторов, одновременно работающих в едином информационном пространстве
- возрастают требования к оперативности принятия решений
- иерархическое управление обусловило повышение роли и ответственности операторов-руководителей
- увеличилась необходимость учета условий труда на рабочих местах операторов
- увеличилась многовариантность: технологий реализации функций, способов выполнения отдельных операций, закрепления операторов за заявками (операциями)
- возрастает цена ошибок

Несмотря на колоссальные достижения в области автоматизации исключить человека из контура управления сложными системами не удается[1-3].

Парадоксально, но роль человека оператора не только не уменьшается, но даже увеличивается. 80% аварий в производственных системах разных типов, более 64% катастроф на морском флоте и 80% в авиации вызваны ошибками человека-оператора[1-3].

Фактически все исследования в области проектирования человеко-машинных систем (ЧМС) ставят целью уменьшить ошибочные реакции человека-оператора [1-5].

Достижения многих исследователей человеческого фактора, направленные на обеспечение безошибочности, наиболее удачно комплексированы в функционально-структурной теории (ФСТ) эрготехнических систем школы проф. А.И. Губинского [4].

В основу этих моделей положены структуры алгоритмов функционирования (АФ) ЧМС и вероятностные характеристики операций этих алгоритмов.

Разработанные в рамках школы ФСТ проф. Губинского А. И. модели выгодно отличаются от многих других [4]:

- ориентацией на количественную оценку
- возможностью редукции («сворачивания») модели АФ с одновременным расчетом прагматических показателей АФ
- компьютерноориентированными зависимостями

Постановка задачи.

Целью настоящей работы являются:

- разработка подхода к решению оптимизационной задачи АФ ЧМС
- содержательный анализ задач, стоящих перед проектировщиками автоматизированных систем по использованию модели для повышения эффективности автоматизированного управления сложными системами.

Подход к решению оптимизационной задачи.

Разработка требований к модели. Оптимизационная модель должна:

- позволять выбирать варианты реализации алгоритмов исполнительской деятельности различных типов независимо от предметной области и содержания выполняемых действий и операций
- быть компьютерноориентированной
- допускать возможность простой реализации на распространенных программных средствах без длительного обучения эргономистов
- допускать возможность создания библиотек типовых моделей для оптимизации наиболее распространенных видов взаимосвязей между операциями АФ
- допускать совместимость при реализации на компьютере с процедурами расчета исходных данных для оптимизации и справочниками по характеристикам качества выполнения типовых действий и операций операторами цифровых систем управления

В связи с тем, что последней наиболее современной средой моделирования ЧМС определена среда EXCEL, в которой разработана информационная система, ориентированная на оценку показателей эффективности реализаций АФ ЧМС (автор- Пасько Н.Б.), в качестве наиболее удобной среды решения оптимизационной задачи также выбраны электронные таблицы.

Таким образом, для решения задачи предложено:

- осуществить переход от графа работ, описывающего АФ ЧМС, к графу событий (полумарковский процесс)
- построить целевую функцию, соответствующую максимизации вероятности поглощения в заданную вершину (безошибочное выполнение)
- сконструировать ограничения (как правило, на время и расход ресурсов)
- реализовать процедуру «Поиск решения»
- проанализировать решение и разработать соответствующие технические решения, реализующие рекомендуемые параметры ЧМС

Разработанное программное и методическое обеспечение максимально упрощает технологию получения оптимальных решений. При этом разработана база данных методов решения типовых задач для типовых АФ ЧМС.

Анализ проблем использования оптимизационных моделей и пути совершенствования эргономических решений. В процессе разработки мероприятий программы обеспечения эргономического качества автоматизированных систем необходимо решать задачи [4]:

- профессиональный отбор операторов
- Выбор степени автоматизации
- распределение функций между операторами
- проектирование информационных моделей
- проектирование условий труда на рабочих местах операторов
- проектирование алгоритмов деятельности

Таким образом, основная проблема проектирования и эффективной эксплуатации автоматизированных систем, стоящая сегодня, - проблема учета всего комплекса влияющих факторов, таких как:

- конструктивные особенности рабочих мест, особенности интерфейса
- напряженность деятельности
- функциональное состояние оператора
- состояние среды
- типовые условия деятельности
- подготовленность оператора
- эмоциональное состояние
- мотивация
- установки (на скорость, на быстродействие) и т.п.

Понятно, что изменение значения любого из указанных факторов приводит к изменению значений эффективности АФ.

Однако, если проанализировать опыт использования в эргономике математических моделей описанного типа, то можно прийти к выводу, что такой опыт имеет место только в рамках научной школы «Эффективность, качество и надежность эрготехнических систем проф. Губинского А. И.»[4]. Среди таких моделей – модели для проектирования алгоритмов деятельности [4,5,6], распределения функций между человеком и автоматикой[4], распределения функций между операторами[4,7,8] и др.

Очевидно, практика эргономического обеспечения редко обращается к оптимизационным моделям эргономики в связи с «узкой трактовкой» понятия «способ выполнения операции». Традиционно в эргономике такой способ трактовался узко (например, «нажать кнопку» или «переключить тумблер» или «дать голосовую команду»).

На практике изменение любого параметра в ЧМС приводит к изменению характеристик способов выполнения операций. Так, например, если решается задача проектирования условий труда на рабочих местах операторов, то соответственно изменяются и надежностно-временные характеристики операций, выполняемых на соответствующих рабочих местах.

Аналогичным образом могут формироваться множества возможных способов выполнения операций посредством учета влияния всех перечисленных выше влияющих факторов. А это – комбинаторная задача.

Очевидно, чтобы преодолеть очевидные трудности применения оптимизационных моделей в эргономике, необходимо:

- расширить трактовку понятия «способ выполнения операции»
- разработать информационную технологию генерации возможных способов выполнения операций на основе комбинации возможных параметров СЧМ.

Библиографический список

1. Rothmorea, P., Aylwardb, P., Karnona J. The implementation of ergonomics advice and the stage of change approach [Text]. / P. Rothmorea, P. Aylwardb, J. Karnona // Applied Ergonomics. – 2015. – № 51. – P. 370–376.
2. Bentley, T.A., Teo, S.T.T., McLeod, L., Tana, F., Bosua, R., Gloet, M. The role of organisational support in teleworker wellbeing: A socio-technical systems approach [Text] / T.A. Bentley, S.T.T. Teo, L. McLeod, F. Tana, R. Bosua, M. Gloet //Applied Ergonomics. – 2016.– № 52.– P. 207–215.
3. Wang, Y., Zheng, L., Hiu, T., Zheng, Q. Stress, burnout and job satisfaction: caseof police force in China [Text] / Y. Wang, L. Zheng, T. Hiu //Public Pers. Manag. – 2014. – №43, – P. 325-339.
4. Информационно-управляющие человеко-машинные системы: исследование, проектирование, испытания: Справочник / Под общ. ред. А.И. Губинского и В.Г. Евграфова. – М.: Машиностроение, 1993. – 528с.
5. Lavrov, E. Modelling Of Operator's Activity In Contact Center Of Providing Internet And Television Services[Text] / E. Lavrov, A. Krivodub, Y. Shapochka // International Scientific Conference «UNITECH '16». Proceedings. 18-19 November 2016, Gabrovo, Bulgaria. - Gabrovo: University Publishing House «V.APRILOV», 2016. – Volume 2. - P.p 195-200.
6. Криводуб А.С. Оценка надежности деятельности операторов в системах предоставления доступа к ресурсам компьютерных сетей //Вісник Національного технічного університету «ХПІ». Серія: Нові рішення у сучасних технологіях. – 2016. – №.18 (1190). – С.140-147.
7. Lavrov, E. Mathematical models for the distribution of functions between the operators of the computer-integrated flexible manufacturing systems / N. Pasko, A. Krivodub, A. Tolbatov // proceedings of the XIII-th international conference tcset'2016 «modern problems of radio engineering, telecommunications, and computer science». – Lviv-Slavsko, Ukraine, february 23 – 26, 2016. – p. 72-76.
8. Lavrov, E. Ergonomics of IT outsourcing. Development of a mathematical model to distribute functions among operators [Text] / E. Lavrov, N. Pasko, A. Krivodub, N. Barchenko, V. Kontsevich //Eastern European Journal of Enterprise Technologies. 2016. – N.4 (80). – P. 32-40.


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАТИКА,
МАТЕМАТИКА,
АВТОМАТИКА
IMA :: 2018
МАТЕРІАЛИ
та програма
НАУКОВО-ТЕХНІЧНОЇ
КОНФЕРЕНЦІЇ
(Суми, 05-09 лютого 2018 року)
Суми,
Сумський державний університет
2018

Аналіз проблем людського фактору в задачах забезпечення кібербезпеки

Щербань Т.В, *студент*; Кіншаков Е.В. *студент*; Лавров Е.А., *професор*
Сумський державний університет, м. Суми

Проблеми кібербезпеки, набули надзвичайної актуальності. Інформаційна безпека (ІБ) складається з цілого комплексу різних заходів і дій. Це, перш за все, контроль дій різного роду суб'єктів - рядових співробітників компанії, привілейованих користувачів, IT-аутсорсерів, контрагентів. Крім того, це чітке розмежування прав доступу всередині компанії, використання резервного копіювання даних, а також наявність простої, зрозумілої і доведеної до відома працівників політики безпеки. У поточних реаліях захист повинен бути досить гнучким, щоб забезпечити і достатній рівень захищеності, і виконання бізнес-цілей. Згідно з інформацією, яка міститься в дослідженні Lloyd's of London і Cyence, фінансові втрати від масштабної кібератаки можуть коштувати світовій економіці від 15,6 млрд до 121 млрд доларів. Якщо розглядати найбільш песимістичний сценарій розвитку подій, то втрати від кібератак можуть перевищити економічний збиток від урагану «Катріна», який став найбільш руйнівним в історії Сполучених Штатів. Втрати від нього склали 108 млрд доларів. У доповіді вказуються два потенційних сценарію розвитку глобальної кібератаки: злом провайдерів хмарних сховищ або використання можливих вразливостей в операційних системах.

У першому сценарії хакери модифікують «гіпервизор», керуючу систему хмарних сховищ, в результаті чого всі зберігаються файли виявляються загубленими. У другому варіанті розглядається гіпотетичний випадок, коли кібераналітік випадково забуває в поїзді сумку, в якій зберігається доповідь про уразливість всіх версій операційної системи, встановленої на 45% всіх світових пристроїв. Ця доповідь згодом продається кримінальним групам. Мінімальний збиток при першому сценарії складе від 4,6 млрд до 53,1 млрд доларів. При другому сценарії втрати складуть від 9,7 млрд до 28,7 млрд доларів.

Людський фактор. Саме проблема «надійних рук» або, кажучи іншими словами, кваліфікованих кадрів є однією з найбільш нагальних. Вона має особливу актуальність протягом усіх останніх років, тому

що на сьогоднішній день людина залишається найбільш уразливим ланкою в IT-інфраструктурі.Найслабша ланка в інформаційній безпеці банку - це співробітник компанії. Якщо співробітники не дотримуються правил безпеки, то технології не зможуть допомогти захиститися.

Так, при використанні соціальної інженерії зловмисники можуть змусити співробітника організації здійснити якусь дію, яке спростить проведення атаки, пояснює експерт. «Часто, щоб підібрати пароль до аккаунту, зловмиснику не обов'язково його« зламувати »- вся інформація про пароль є в профілі соціальних мереж або поруч з робочим столом. Навіть співробітники на керівних позиціях виробляють маніпуляції, спровоковані зловмисниками. Окремим рядком можна привести небажання працівників слідувати політиці і вимогам по ІБ заради спрощення своєї роботи». Щоб мінімізувати вплив людського фактора, потрібно постійно підвищувати обізнаність співробітників в області ІБ, а також впроваджувати систему контролів і моніторингу дотримання політик і вимог в області ІБ. Серед основних способів мінімізації загрози ІБ -підвищення обізнаності персоналу в питаннях ІБ, проведення тестів, ділових ігор, кібернавчань.

У зв'язку з проблемою ризиків, які несе людський фактор, цікаво згадати дослідження антивірусної компанії ESET, опубліковане в липні 2017 року. Чотири компанії з п'яти недооцінюють ризики ІБ, пов'язані з людським фактором. Такий висновок зробили співробітники ESET після опитування інтернет-користувачів з СНД. Респондентам запропонували вибрати відповідь на питання «Чи проходили ви на роботі тренінг з інформаційної безпеки?». Негативна відповідь лідирує з великим відривом. 69% респондентів ніколи не проходили навчання основам кібербезпеки в своїх компаніях. Ще 15% учасників опитування повідомили, що їх роботодавці обмежилися мінімальним обсягом інформації. Навчання не виходило за рамки «в разі неполадок перезавантажте комп'ютер», правила кібербезпеки не зачіпалися. Тільки 16% респондентів пройшли якісні тренінги з докладною розповіддю про інформаційну безпеку. Для порівняння: більше 60% учасників аналогічного опитування в США повідомили, що їх роботодавці організували для них навчання з кібербезпеки.

TECHNICAL UNIVERSITY OF GABROVO

INTERNATIONAL

SCIENTIFIC CONFERENCE

PROGRAM

17 - 18 NOVEMBER 2017
GABROVO

UNITECH 2017 GABROVO

INTERNATIONAL SCIENTIFIC CONFERENCE
17-18 November 2017, GABROVO

A BASIC MODEL OF OPTIMIZATION OF THE MAN - MACHINE INTERACTION AND THE ANALYSIS OF THE PROSPECTS OF ITS USE IN ERGONOMICS OF AUTOMATED SYSTEMS

N.B. Pasko
Sumy National Agrarian University(Ukraine)
E.A. Lavrov, Y.S. Mikhaylenko, T.V. Shcherban
Sumy State University(Ukraine)

Abstract
A mathematical model of optimization of the man-machine system by the description of the functional algorithm in a form of an event graph was worked out.
Keywords: man-mashine system, optimization, algorithm, function,event graph , ergonomics.

INTRODUCTION

Last years are characterized by a rapid change in the nature of automated technology management [1-3]:

- distributed information systems became widely spread;
- the number of operators, working simultaneously in single information space, has increased;
- the requirements for the efficiency of making decision are increasing;
- hierarchical management stipulated an increase of the role and responsibility of management operators;
- the necessity to take into account working conditions at the operator's workplaces has increased;
- the multivariance of technologies for the implementation of functions, ways of performing of individual operations, assigning operators to applications (transactions) has increased;
- the cost of errors is increasing.

In spite of the enormous achievements in the field of automation, it is impossible to exclude a person from management of complicated systems [1-3].

Paradoxically, but the role of the man-operator not only diminished, but it has even increased. 80% of accidents in production systems of different types, more than 64% of accidents in the marine fleet and 80% in aviation are caused by man-operator errors[1-3].

In fact, the purpose of every research in the field of designing of man-machine systems (MMS) is to reduce the mistaken reactions of man-operator [1-5].

The achievements of many researchers of the human factor, aimed at ensuring accuracy, are most successfully integrated in the functional-structural theory(FST) of ergotechnical systems of the school of Professor A.I. Gubinsky[1].

These models are based on the structure of algorithms for the functioning (AF) of MMS and probabilistic characteristics of the operations of these algorithms.

Developed within the framework of the FST schools, the Professor Gubinsky A.I. models stand out from many others by:

- focus on quantitative assessment;
- possibility of reduction ("folding") of the AF model with simultaneous calculation of the pragmatic AF parameters;
- computer-oriented dependencies.

The objectives of this work are:

- the development of the approach to the solution of the optimization problem of the AF MMS
- the substantive analysis of the tasks facing the designers of automated systems for using the model to improve the efficiency of automated control of complex systems.

EXPOSITION

Development of requirements for the model. The optimization model should:

- allow to choose the variants to implement the algorithms of performing activity of various types irrespective of a subject area and the maintenance of carried out actions and operations;
- be computer-oriented
- allow for the simple realization on common software without the long-term training of ergonomists;
- allow for the creating of a library of standard models for the optimization of the most common types of relationships between AF operations;
- be compatible with the procedures of calculating the initial data for optimization and the guides on the performance characteristics of common actions and operations by ACS operators when realized on a computer.

In view of the fact that the latest most modern environment for modeling MMS has been determined the Excel environment, in which it was developed an information system focused on the evaluation of the performance indicators of AF FS implementation (author - Pasko NB), spreadsheets are also chosen as the most convenient environment for solving the optimization problem.

Development of the AF model initial for optimization problem statement.

The functioning of the system can be formulated in the form of a work graph and an event graph.

The work graph represents a logic model of an interaction of the AF operation recorded with the help of special symbols (functionaries, i.e., operations: working procedures, control of functioning, control of efficiency, alternative, etc. [4]).

The event graph is a secondary one and based on the works graph.

"Events" reflect the consequences of performing of AF "works", for example

- "free-error performing of a work operation",
- "performing of a work operation with an error".

An example of the transition from the work graph to the event graph is shown on Picture 1, where the following designations are introduced:

P_i - work operation with number i,

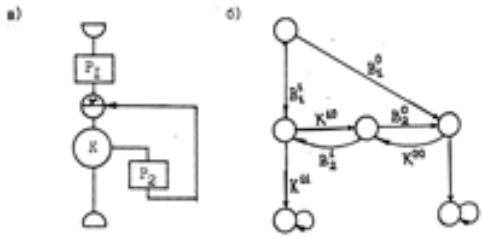
K – performance control operation

$B_i^1(B_i^0)$ - probability of error-free (erroneous) performance of the operation with the number i;

K^{11} - the probability of recognizing that the error-free performance of a work operation is error-free;

K^{00} - the probability of recognizing that the erroneous performance of a work operation is erroneous;

$K^{01} = 1 - K^{00}; K^{10} = 1 - K^{11}$.



Picture 1 - the example of a transition from work graph to the event graph
a) work graph; b) event graph.

Optimization model on the "events" graph.

The use of the work graph for the ergonomist-designer is more convenient and visual, but it is possible to put the optimization problem on it only for particular cases (as a rule, for AF of a sequential type).

In this connection we will develop an optimization model on the "events" graph, which is a semi-Markov process (SMP).

The problem can be reduced to the problem of ensuring the maximum probability of absorption into a given state s, which, for example, corresponds to the event "**error-free execution of AF**".

On the event graph, we will assign our absorption state to each variant of the end of the operation accordingly, for example, "**error-free execution of AF**" or "**execution of an AF with an error**".

The vertices, which correspond to the absorption states, are numbered by the first r natural numbers (r is the number of absorbing vertices of the SMP).

For initial vertices, which are numbered by numbers from the numerical sequence after the first r absorbing vertices, it is necessary to specify a vector of initial probabilities, that is, the probability of finding the system in the initial states at the corresponding vertex of the event graph:

$$a=(a_{r+1},a_{r+2},...,a_m),\ \sum_{i=r+1}^{m} a_i=1$$

Let us introduce the following variables and designations: P_{ij}^k - the probability of the transition of the SMP from the vertex i to the vertex j in the k-th method of performing the work,

N - the total number of vertices, of which the first r - the absorption vertices ,

$\overline{t_i^k}$ - the mathematical expectation of the random variable of process length of stay at the vertex i when choosing the k-th solution,

$\overline{u_i^k}$ - the mathematical expectation of resource consumption when the process is at the vertex i and the k-th solution is chosen;

T_0 - the limitation on AF execution time,

U_0 - the restriction on resource consumption for the implementation of AF,

x_i^k - the variable that characterizes the choice of the solution: $x_i^k>0$ if for i-th vertex is chosen k solution, otherwise i is equal 0,

K_i - the set of admissible solutions in the i-th vertex.

In such conditions, the problem is formulated as follows:

$$\begin{cases}
\sum_{i=r+1}^{N}\sum_{k\in K_i} P_{ij}^k x_i^k \to \max & (1)\\
\sum_{i=r+1}^{N}\sum_{k\in K_i} x_i^k \overline{t_i^k} \le T_0 & (2)\\
\sum_{i=r+1}^{N}\sum_{k\in K_i} x_i^k \overline{u_i^k} \le U_0 & (3)\\
\sum_{k\in K_j} x_j^k - \sum_{i=r+1}^{N}\sum_{k\in K_i} x_i^k P_{ij}^k = a_j,\ j=\overline{r+1,N} & (4)\\
x_j^k \ge 0;\quad j=\overline{r+1,N};\quad k\in K_j & (5)\\
\sum_{k\in K_j}\delta_j^k = 1 & (6)\\
x_j^k - M\delta_j^k \le 0,\ j=\overline{r+1,N};k\in K_j & (7)\\
\delta_l^k=\delta_m^k=...=\delta_n^k, k\in K_j; & (8)
\end{cases}$$

where $l,m,...,n$ - dependent states which correspond to one AF operation (there may be several vertices on the event graph of one operation and it is obvious that identical decisions must be taken for them) or to the different operations that must be performed in the same way; δ_i^k - a boolean variable (it takes the value 0 or 1); M - a sufficiently large number.

The conditions (6) and (7) are required to find the unique solution at the vertex where the only one way of performing the operation is admissible. As in the ACS in each particular operation mode, each operation can be performed only in the one way, and change of the way is possible only when another mode has been chosen and for each mode it is necessary to build the appropriate AF, we will use only a pure strategy. So, the restriction of type (6) and (7) shall be introduced for all vertices. The restriction (8) is required for choosing the same solutions in dependent states.

The convenience of the model (1) - (7) is that the problem is reduced to the problem of linear programming, which can be solved with the help of any software package focused on this problem.

Approbation. We carried out wide approbation of models of this type in different software environments, including:

- Excel
- Matlab.

The model has been used many times in solving problems of ergonomic design:

- Call-centers [5]
- Systems which provide access to Internet resources [6]
- Flexible manufacturing systems [7]
- Outsourcing campaign management systems [8-9]
- Management of the main gas pipeline [10-11]
- Settlement centers [12]
- e-learning [13]
- Production processes of machine-building enterprises [14-15], chemical industry enterprises [16].
- And etc.

Analysis of the problems of the ergonomic management of the optimization model.

In the process of the development of the arrangements for ergonomic quality assurance programs of automated systems it is required to solve the following tasks [4]:

- Professional selection of operators
- Selecton of the degree of automation
- Distribution of functions between operators
- Design of information models
- Design of working conditions at operator's workplaces
- Design of the activity algorithms.

So far the main problem of the designing and efficient operation of ACS is to take into consideration the whole complex of influencing factors, such as:

- design features of workplaces, interface features;
- the intensity of activities,
- operator's functional state,
- the state of the environment,
- temporal conditions of activity,
- qualification of an operator,
- emotional condition,
- motivation,
- settings (for speed, response time, etc.)

It is clear that a change in the value of any of these factors leads to a change in the value of effectiveness of the AF.

However, analyzing the experience of using mathematical models of the type (1) - (8) in ergonomics, it is possible to make the conclusion that such an experiment takes place only within the framework of the scientific school "Efficiency, quality and reliability of ergotechnical systems of professor Gubinsky A.I. "[4-17]. Among such models there are the models for the design of activity algorithms [4,5,6,9,17], the distribution of functions between a human and automation [4], the distribution of functions among operators [4,7,11,12], etc

Obviously, the practice of ergonomic management rarely refers to models of the type (1) - (8) because of the "narrow interpretation" of the concept "the method of performing an operation" (from the set of K_l - admissible solutions at the l-th vertex – refer to tasks (1) - (8)). Traditionally in ergonomics such method is interpreted restrictively (for example, " to press the button" or " to toggle" or "to give a voice command")

In practice, the change of any parameter in the MMS leads to a change of the characteristics of the ways of operation performance. So, for example, if it is solved the problem of the design of working conditions at the operators' workstations is solved, then the reliability and time response characteristics of the operations performed at the corresponding work places are also changed accordingly.

Likewise there can be formed the variety of possible ways of the performing of operations taking into consideration the influence of all the above-mentioned influencing factors. And this is a combinatorial problem.

Evidently to overcome the obvious difficulties of applying optimization models in ergonomics it is required:

- to expand the interpretation of the concept of " the method of operation performance"
- to develop information technology to generate possible ways of performing operations based on a combination of possible MMS parameters

CONCLUSION

It has been developed the mathematical model of the optimization of the human-machine system when describing the algorithm of functioning in the form of an event graph.

The optimization is reduced to the problem of linear programming.

The wide outreach of information technologies for solving linear programming problems makes this model quite a convenient tool for ergonomists and experts in the reliability of MMS.

The task of the subsequent widespread implementation of the optimization model in ergonomic management of automated systems is determined as the task of automatic generation of the alternatives for AF MMS. operations with the determination of the appropriate reliability and time response characteristics.

REFERENCES:

[1] Rothmorea, P. , Aylwardb, P., Karnona J. The implementation of ergonomics advice and the stage of change approach [Text]. / P. Rothmorea , P. Aylwardb, J. Karnona // Applied Ergonomics. – 2015. – № 51. – P. 370–376.

[2] Bentley, T.A., Teo, S.T.T., McLeod, L., Tana, F., Bosua, R., Gloet, M. The role of organisational support in teleworker wellbeing: A socio-technical systems approach [Text] / T.A. Bentley, S.T.T. Teo, L. McLeod, F. Tana, R. Bosua, M. Gloet //Applied Ergonomics.– 2016.– № 52.– P. 207–215.

[3] Wang, Y., Zheng, L., Hiu, T., Zheng, Q.Stress, burnout and job satisfaction: caseof police force in China [Text] / Y. Wang, L. Zheng, T. Hiu //Public Pers. Manag. – 2014. – №43, – P. 325-339.

[4] Gubinskiy A.I., Evgrafov V.G. Information controlling human-machine systems: research, design, testing. Reference book, Moscow, Mechanical Engineering, 1993. 528 p. (In Russian)

[5] Lavrov, E. Modelling Of Operator's ActivityIn Contact Center Of Providing Internet And Television Services[Text] / E. Lavrov, A. Krivodub, Y. Shapochka // International Scientific Conference "UNITECH '16". Proceedings. 18-19 November 2016, Gabrovo, Bulgaria. - Gabrovo: University Publishing House "V.APRILOV", 2016. – Volume 2. - P.p 195-200

[6] Krivodub A.S. Evaluation of the reliability of operators' activity in systems providing access to computer network resources. Series: New solutions in modern technologies. News of National Technical University "KhPI", 2016, no. 18 (1190), pp. 140-147. (In Russian)

[7] Lavrov, E. Mathematical models for the distribution of functions between the operators of the computer-integrated flexible manufacturing systems / N. Pasko, A. Krivodub, A. Tolbatov // proceedings of the XIII-th international conference tcset'2016 "modern problems of radio engineering, telecommunications, and computer science". – Lviv-Slavsko, Ukraine ,february 23 – 26, 2016. – p. 72-76

[8] Lavrov, E. Ergonomics of IT outsourcing. Development of a mathematical model to distribute functions among operators [Text] / E. Lavrov, N. Pasko, A. Krivodub, N. Barchenko, V. Kontsevich //Eastern European Journal of Enterprise Technologies. 2016. – N4 (80). – P. 32-40

[9] Lavrov E.A., Krivodub A.S. The approach to the evaluation of options for the operators of technical support for information services of telecommunication systems. Reports of BSUIR, Minsk, 2015, no. 2 (88), pp. 123-126. (In Russian)

[10] Koshara V.S., Lavrov E.A. The formalized description of the activity of operators of the gas-pumping plant control system // Computer science, mathematics, automatics: the materials and the program of the scientific and technical conference, Sumy, April 18-22, 2016 .- Sumy, Sumy State University, 2016, 96 p. (In Russian)

[11] Koshara V., Krivodub A.,Pasko, N., Lavrov E. Information Technology Distribution of Applications between Operators of the Compressor Station //Advanced Information Systems and Technologies : proceedings of the IV international scientific conference, May 25-27, 2016 - Sumy: Sumy State University, 2016. - P. 89

[12] Lavrov, E. Information technology for distribution of functions between operators in automated systems. Analysis of efficiency. [Text] / E. Lavrov, N. Pasko, // International Scientific Conference "UNITECH '15". Proceedings.18-19 November 2015, Gabrovo, Bulgaria. - Gabrovo: University Publishing House "V.APRILOV", 2015. – Volume 2. - P.p 298-306

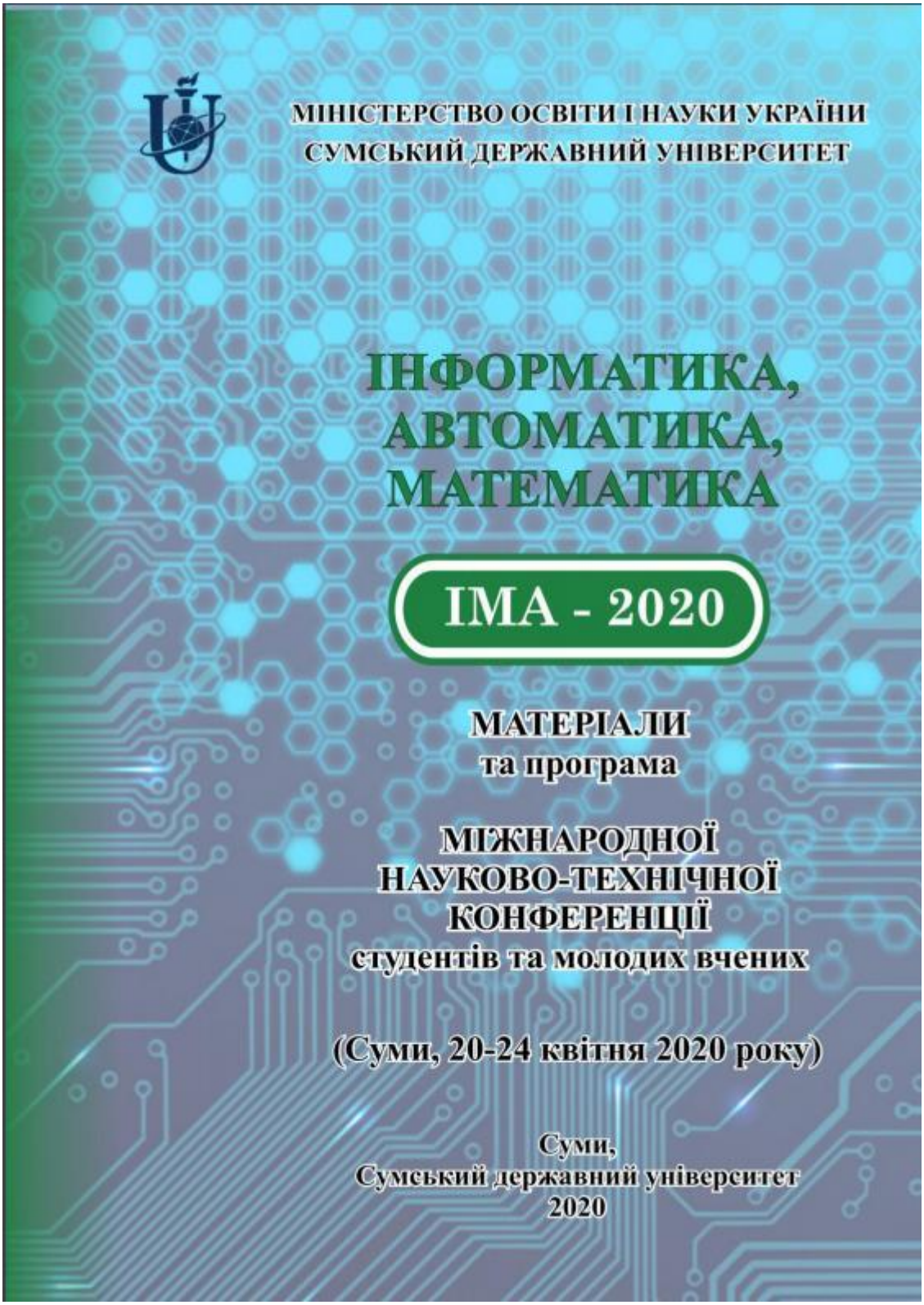
[13] Lavrov E. Development of models for the formalized description of modular e-learning

systems for the problems on providing ergonomic quality of human-computer interaction/ E Lavrov, N Barchenko, N Pasko, I Borozenec// Eastern-European Journal of Enterprise Technologies 2 (2 (86)), 4–13

[14] Bahmach M., Lavrov E. Program Complex of Statistical Calculations for Control the Quality of Products at Lebedinsky Plant of Piston Rings Advanced Information Systems and Technologies: proceedings of the IV international scientific conference, May 25-27, 2016– Sumy: Sumy State University, 2016. – P. 82-84

[15] Bakhmach N.V., Lavrov E.A. The formalized description of the production processes at the Lebedinsky Factory of Piston Rings for quality management tasks // Computer science, mathematics, automatics: the materials and the program of the scientific and technical conference, Sumy, April 18-22, 2016 – Sumy, Sumy State University, 2016, 90 p. (In Russian)

[17] Lavrov E.A., Skidanenko A.S. Ergonomic reserves of increasing the efficiency of automated process control system for the production of fertilizers // Modern Information Systems and Technologies: the materials of the Second International Scientific and Practical Conference, Sumy, May 21-24, 2013 - Sumy: Sumy State University, 2013, pp. 53-54. (In Russian)


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАТИКА, АВТОМАТИКА, МАТЕМАТИКА
ІМА - 2020
МАТЕРІАЛИ
та програма
МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ
студентів та молодих вчених
(Суми, 20-24 квітня 2020 року)
Суми,
Сумський державний університет
2020

Моделі функціонування інформаційної системи без та із засобами захисту інформації в умовах конфліктної взаємодії

Щербань Т.В., *студентка*; Лавров Є.А., *професор*
Сумський державний університет, м. Суми, Україна

Математична модель конфлікту системи з негативним впливом грунтується на поданні процесу зміни станів об'єднаної системи у вигляді ланцюга Маркова з кінцевим числом станів, переходи між якими здійснюються за експоненціальним законом розподілу.

На рисунку 1 представлені стани, в яких може перебувати джерело негативного впливу при підготовці і проведенні негативного впливу на інформаційну систему БЕЗ засобів захисту інформації, а також можливі переходи з одного стану в інший.

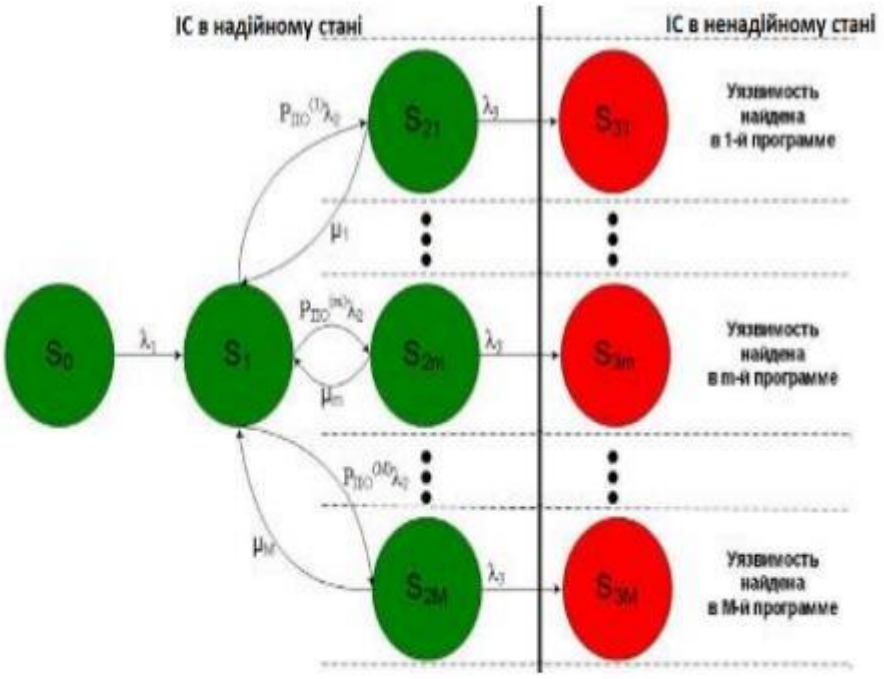


Рисунок 1 – Математична модель конфлікту без засобів захисту

Для того, щоб врахувати в математичній моделі конфлікту засоби захисту інформації, необхідно внести зміни, а саме додати стани, що відображають розвідку негативного впливу про засоби захисту системи, а також переходи в стани, що відповідають наявності інформації про засоби захисту інформаційної системи, з усіх наступних станів.

Даний процес зображений на рисунку 2.

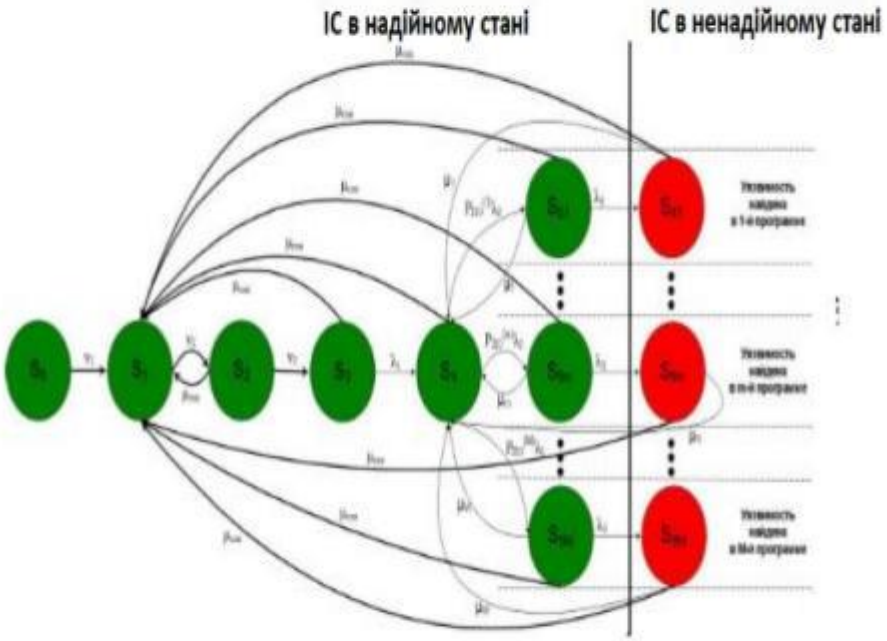


Рисунок 2 – Математична модель конфлікту із засобами захисту

Розроблені математичні моделі конфлікту дозволяють враховувати різний склад і структуру побудови інфомаційної системи (наявність різного програмного забезпечення, наявність засобів захисту і т.п.); динаміку вразливостей і вплив на надійність системи роботи адміністратора; різні варіанти конфліктів, засновані на реальних ситуаціях.

Оптимізація розподілу заявок в системах технічного супроводу інформаційних систем

Щербань Т.В., *студентка*; Гаврилів А.О., *студентка*;
Лавров Є.А., професор
Сумський державний університет, м. Суми, Україна

Основна проблема існуючих алгоритмів оптимізації є вирішення задачі з обмеженням на середній час виконання. Дослідження показали, що при даних умовах вже не можна розглядати час як постійну величину, і тому вони дають помилковий результат. До цього часу не реалізовані алгоритми оптимізації, які сприймають час як ймовірнісну величину, що в свою чергу може значно підвищити ефективність. У такому випадку математична модель в загальному вигляді має наступний вигляд:

$$\begin{cases} B(\mathrm{X}) \to max \\ P\{T(\mathrm{X}) \le T_0\} \ge \theta_0 \\ X \in X' \\ U(\mathrm{X}) \le U_0 \end{cases},$$

– максимізація ймовірності безпо-милкового виконання, X – спосіб виконання операції, заміна обмеження на математичне сподівання на ймовірність своєчасного виконання: $P\{T(\mathrm{X}) \le T_0\} \ge \theta_0$, $T(\mathrm{X})$ – випадкова величина часу виконання, θ_0 - мінімальна ймовірність своєчасного виконання, U(X) – витрати ресурсів при даному способі виконання. U_0 – задана кількість ресурсів. X' – ОДР задачі оптимізації. Найбільш проста процедура такого рішення, орієнтована на наявний метод вирішення детермінованою завдання виглядає наступним чином. 1. Пошук оптимального рішення на детермінованою моделі АФ (рішення задачі без урахування імовірнісного обмеження на час виконання АФ, а з обмеженням на математичне очікування часу виконання АФ):

$$\sum_{i=r+1}^{N} \sum_{k \in k_i} \overline{t_i^k} \le T_0$$

2. Визначення функції розподілу часу виконання АФ і ймовірності своєчасного виконання АФ для отриманого рішення і, якщо вона відповідає умові - зупиниться (отримано оптимальне рішення), якщо немає - коригування ОДР (образно кажучи - знаходження «кордону відходу»).

3. Рішення детермінованою завдання в новій ОДР.

Кордон відходу можна знайти наступним чином. Разом з тим, в розробленому вигляді не всі можливості розглянутого походу вичерпані. Це пов'язано з прийнятим припущення про незмінність функції розподілу часу

реалізації АФ для рішень, отриманих на етапі 1 і етапі 3. Таке припущення може викликати або недотримання , образно кажучи, «недоліт» при визначенні T_po; або при дотриманні виявлення рішення, що не гарантує максимальну ймовірність безпомилкового виконання АФ («переліт»). Зняти це припущення можна за допомогою послідовного уточнення кордону функціонального обмеження, коли кожен раз після знаходження рішення детермінованою завдання досліджується функція розподілу часу виконання АФ і знаходиться «кордон відходу» і так до отримання гарантованого із заданою точністю результату. Така послідовна корекція «кордону відходу» ускладнює пошук оптимуму, але дозволяє виявляти додаткові резерви підвищення безпомилковості функціонування ЕТС. З міркувань практики для скорочення кількості ітерацій необхідно передбачити завершення процедури не тільки в разі отримання оптимального рішення, але і в разі отримання допустимого рішення зі значенням цільової функції, що відрізняється від максимально можливого при заданих обмеженнях не більше, ніж на деяку певну величину ε. Таким чином, гарантується здобуття оптимального рішення. Алгоритм можна представити у вигляді схеми(рис. 1), яка демонструє які дії повторюються, число умов та циклів, критерій зупинки роботи та для полегшення створення інформаційної системи, при написанні основного коду програми.

Рисунок 1 – Загальна схема алгоритму оптимізації

Алгоритм оптимізації з обмеженням по вірогідності доцільно організовувати таким чином, щоб: вирішувати детерміновану задачу, оцінювати вірогідність своєчасного виконання, корегувати область допустимих рішень.

Моделювання конфлікту інформаційної системи з наявними в ній джерелами негативного впливу

Щербань Т.В., *студентка*; Ніколаєнко К.О., *студентка*;
Лавров Є.А., професор
Сумський державний університет, м. Суми, Україна

Програмне забезпечення, яке встановлене в інформаційній системі, представляє собою операційну систему, а також різні утиліти та прикладні програми, особливістю яких є наявність малої кількості вразливостей. Існуючі моделі конфлікту інформаційної системи і джерела негативного впливу враховують тільки середнє значення середньостатистичного числа вразливостей за період конфлікту, тоді як в реальності середньостатистичне число вразливостей протягом цього періоду може змінюватися. Крім того, реально розподіл часу переходів в різні стани може носити довільний, що відрізняється від пуассонівської моделі, характер. Також, часто виникає необхідність розглядати ситуацію, що принципово відрізняється від дуельної, коли конфлікт зачіпає кілька учасників з кожного боку (наприклад, інформаційну систему атакують не один, а кілька джерел негативного впливу). Необхідність врахування всіх значущих для опису інформаційного конфлікту чинників неминуче ведуть до зростаючих труднощів при використанні аналітичних математичних моделей. Це визначає істотну роль засобів і комп'ютерних технологій об'єктно-орієнтованого моделювання для дослідження закономірностей конфлікту. Одним з доступних комп'ютерних засобів і природним для опису динаміки ситуаційного конфлікту механізмом реалізації комп'ютерних імітаційних моделей інформаційного конфлікту систем є використання формалізму гібридних автоматів (карт станів Харела) і тих можливостей, які для цих цілей надає інтегроване середовище MATLAB + Simulink + Stateflow, в якому і була створена імітаційна модель конфлікту інформаційної системи без засобів захисту інформації та джерела негативного впливу. За допомогою даної моделі можна розрахувати ймовірність надійності ІС протягом певного часу, тобто ймовірність непотрапляння ІС в «ненадійний стан» протягом цього часу, і ймовірність знаходження ІС в «надійному стані» протягом певного часу.

Модель у середовищі Simulink продемонстрована на рисунку 1.

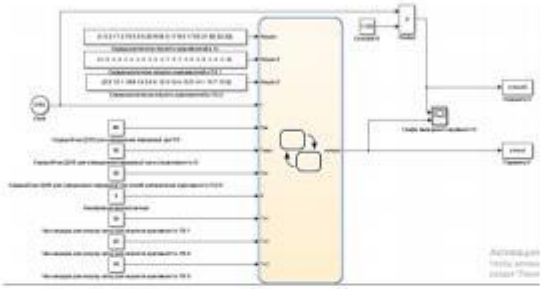


Рисунок 1 – Імітаційна модель конфлікту

Конфліктну взаємодію можна описати за допомогою SF-моделі (рис. 2), яка складається з 3-х паралельно функціонуючих об'єктів («Sysadmin» і «IS» з одного боку, «INV» з іншого боку), в яких розміщені карти станів, що описують можливі значення чинників, що враховуються і поведінку всіх сторін, що беруть участь в конфлікті.

Рисунок 2 – SF-модель конфлікту інформаційної системи

На відміну від моделей конфлікту, в представленій моделі жодна зі сторін не може досягти абсолютної перемоги, тобто в разі переходу інформаційної системи в ненадійний стан, вона може знову повернутися в захищений стан (відновитися). Тому в ході експерименту крім розрахунку числа перемог сторін конфлікту (наприклад, ймовірність того, що інформаційна система за період конфлікту не перейде в ненадійний стан), може бути також розрахована ймовірність знаходження сторін конфлікту в певному стані (наприклад, ймовірність знаходження інформаційної системи в надійному стані).

Оптимізація діяльності операторів для забезпечення ергономічної якості інформаційних систем

Щербань Т.В., *студентка*; Овчаренко К.В., *студентка*;
Лавров Є.А., професор
Сумський державний університет, м. Суми, Україна

Задача "розподіл функцій між операторами" є традиційною задачею ергономіки, однак, незважаючи на великий науковий доробок, існуючі моделі не можуть бути застосовані для сучасних систем, оскільки заявки надходять у випадкові моменти часу і необхідно враховувати індивідуальні особливості операторів, що працюють в системі. Задача має вирішуватися багаторазово і може бути актуальною в довільний момент часу. У загальному випадку математична модель оптимізаційної задачі має вигляд:

$$F(X) \to \min, \quad (1)$$

$$Q(X)\,\theta\,Const, \quad (2)$$

$$X \in X', \quad (3)$$

де X – вектор, що задає варіант закріплення оператора за заявкою (функцією); F (X) – цільова функція, що виражає величину збитку від можливих помилок операторів при виконанні заявок; Q (X) – вектор, який характеризує систему обмежень; θ – операції порівняння (=,>, <,> =, <=); Const – вектор констант; X' – область допустимих рішень, яка формується виходячи з аналізу можливостей, функціонального стану, зайнятості, напруженості діяльності операторів і інших можливих чинників. Оптимізація алгоритмів функціонування може бути проведена з використанням двох можливих уявлень процесів людино-машинного взаємодії: на графі робіт і з використанням графа можливих подій (рис. 1).

а б

Рисунок 1 – Приклад формального опису АФ:
а - граф робіт; б - граф подій.

Розроблено спосіб для випадку опису алгоритму функціонування у вигляді графа подій, який, незважаючи на складність формування моделі, володіє великими можливостями (в порівнянні з оптимізацією на графі робіт, яка зручна виключно для алгоритму функціонування послідовного типу). Задача оптимізації людино-машинного взаємодії зводиться до пошуку стратегії поглинаючого ПМП, що забезпечує максимум ймовірності поглинання процесу в стан r, що відповідає реалізації АФ "без помилки". Модифікуємо цю модель таким чином, щоб вирішити поставлену задачу призначення операторів на функції і у підсумку отримаємо наступний вигляд оптимізаційної моделі:

$$\sum_{z=1}^{Z}((1-\sum_{h}\sum_{i^z=r^z+1}^{N^z}\sum_{k\in K}P_{i^z1}^{(k)}\cdot x_{i^z}^{(k)})\cdot U^z+(\sum_{j^z=r^z+1}^{N^z}\sum_{j^z}\sum_{k\in K}P_{i^z1}^{(k)}\cdot x_{j^z}^{(k)})\cdot u^z)\to\min$$

$$\sum_{k\in K}x_{j^z}^{(k)}-\sum_{i^z=r^z+1}^{N^z}\sum_{k\in K}P_{i^zj^z}^{(k)}\cdot x_{i^z}^{(k)}=a_{j^z}^z,\ j^z=r^z+1,r^z+2,\ldots,N^z,\ \forall z\in Z,$$

$$\sum_{j^z=1}^{r^z}\sum_{i^z=r^z+1}^{N^z}\sum_{k\in K}P_{i^zj^z}^{(k)}\cdot x_{i^z}^{(k)}=1,$$

$x_{j^z}^{(k)}\ge 0$ при всіх j^z і всіх $k\in K$,

$$\sum_{i=r^z+1}^{N^z}\sum_{j^z}\sum_{k\in K}P_{i^zj^z}^{(k)}\cdot T_{i^zj^z}^{(k)}\cdot x_{i^z}^{(k)}\le T_0^z \quad \text{при всіх} \quad z\in Z,$$

$\sum_{k\in K}\delta_z^{(k)}=1$ для всіх z,

$x_{j^z}^{(k)}-M\cdot\delta_z^{(k)}\le 0$ при всіх j^z і всіх $k\in K$,

$x_{j^z}^{(k)}-m\cdot\delta_z^{(k)}\ge 0$ при всіх j^z і всіх $k\in K$,

$\sum_{z\in Z}\delta_z^{(k)}\le 1$ при всіх $k\in K$. |

Розроблена модель дозволяє вирішувати задачу оптимального розподілу заявок, що надходять у випадкові моменти часу на реалізацію дискретних функцій між операторами. Забезпечується мінімізація шкоди від ненадійних дій операторів і виконання обмежень на своєчасне виконання.Переваги розробки полягають у тому, що рішення приймаються на основі кваліметричного підходу і їх характеристики можуть бути оцінені кількісно, при цьому забезпечується можливість обліку структур діяльності операторів, а також індивідуальних характеристик їх надійності та швидкодії. При традиційному закріпленні операторів за заявками, що виконуються, як правило, на підставі інтуїції керівників в умовах обмеженого часу, якість прийнятих рішень не може бути гарантовано.

ДОДАТОК Д КОПІЇ ГРАМОТ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ДИПЛОМ

III СТУПЕНЯ

нагороджується

Щербань Тетяна Володимирівна

студентка Сумського державного університету

ПЕРЕМОЖЕЦЬ

другого туру Всеукраїнського конкурсу студентських наукових робіт з галузей знань і спеціальностей у 2018/2019 навчальному році за спеціальністю «Кібербезпека»

Голова галузевої конкурсної комісії,
проректор з науково-педагогічної роботи О.М. Новіков

05 квітня 2019 р.

Міністерство освіти і науки України

Вінницький національний технічний університет

Дипломом переможця 3 ступеня нагороджується

ЩЕРБАНЬ

Тетяна Володимирівна

Сумський державний університет

Всеукраїнський конкурс
студентських наукових робіт з напрямку
«Інформатика і кібернетика»

Вінниця 12-13 квітня 2018 р.

Голова конкурсної комісії,
проректор з наукової роботи ВНТУ, д.т.н., проф. С. В. Павлов

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ДИПЛОМ

III СТУПЕНЯ

нагороджується

Щербань Тетяна Володимирівна

студентка Сумського державного університету

ПЕРЕМОЖЕЦЬ

II туру Всеукраїнського конкурсу студентських наукових робіт з галузей знань і спеціальностей у 2017/2018 навчальному році за спеціальністю «Кібербезпека»

Голова галузевої конкурсної комісії,
проректор з науково-педагогічної роботи *О.М. Новіков*
27 квітня 2018 р.

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ХНУ

ГРАМОТА

нагороджується

Щербань Тетяна
Плеханов Євгеній

студенти
Сумського державного університету

Науковий керівник - професор Лавров Є.А.

за 2 місце

у II турі Всеукраїнського конкурсу
студентських наукових робіт з
Інформаційних технологій

Ректор Скиба М.Є.

м. Хмельницький
2019 рік

Міністерство освіти і науки України

Вінницький національний технічний університет

Дипломом переможця "___" ступеня нагороджується

Щербань Тетяна Володимирівна
Ніколаєнко Кароліна Олександрівна

Сумський державний університет

Всеукраїнський конкурс
студентських наукових робіт з напрямку
"Інформатика та кібернетика"

Вінниця 11-12 червня 2020 р.

Голова конкурсної комісії,
проректор з наукової роботи ВНТУ, д.т.н., проф. С. В. Павлов