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

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему: «Комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій»

за напрямом підготовки 6.050101 «Комп'ютерні науки»

Виконавець роботи: студент групи ІТ-51 Щербань Тетяна Володимирівна

Кваліфікаційна робота бакалавра
захищена на засіданні ЕК
з оцінкою _____«__» _____2019 р.

Науковий керівник _____ _____д.т.н., проф. Лавров Є.А.____
(підпис) (науковий ступінь, вчене звання, прізвище та ініціали)

Голова комісії _____ _____Шифрін Д.М._____
(підпис) (науковий ступінь, вчене звання, прізвище та ініціали)

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

Студент _____
(підпис)

Суми-2019

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
«__» _____ 2019 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА СТУДЕНТУ

Щербань Тетяна Володимирівна

1 Тема роботи *Комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій*

керівник роботи *Лавров Євгеній Анатолійович, д.т.н., професор*,

затверджені наказом по університету від « 17 » травня 2019 р. № 084-III

2 Строк подання студентом роботи «10» червня 2019 р.

3 Вхідні дані до роботи
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, які потрібно розробити)
Аналіз процесу виявлення та усунення вразливостей, мета та постановка задачі, математична модель функціонування інформаційних систем в умовах внутрішніх вразливостей і конфліктних взаємодій, об'єктно-орієнтовані моделі конфліктної взаємодії, розробка імітаційної моделі конфлікту інформаційної системи і джерела негативного впливу.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) _____

Актуальність, апробація, аналіз процесу виявлення та усунення вразливостей, постановка задачі, розроблення математичних, об'єктно-орієнтованих моделей, розроблення імітаційної моделі, порівняння результатів математичної та імітаційної моделей, впровадження, висновки.

6. Консультанти розділів роботи:

Розділ	**Консультант**	**Підпис, дата**	
		Завдання видав	**Завдання прийняв**

7.Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Ідентифікація ідеї проекту	15.04.19-16.04.19	
2	Аналіз процесу виявлення та усунення вразливостей в інформаційних системах	17.04.19-19.04.19	
3	Постановка задачі та планування робіт	23.04.19-30.04.19	
4	Розробка математичної моделі	01.05.19-14.05.19	
5	Розробка об'єктно-орієнтованих моделей	15.05.19-21.05.19	
6	Розробка імітаційної моделі	20.05.19-31.06.19	
7	Створення документації	23.04.19-03.06.19	
8	Здача пояснювальної записки	10.06.19	
9	Презентація проекту	18.06.19	

Студент _____ Щербань Т.В.
(підпис)

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

РЕФЕРАТ

Тема бакалаврської роботи: «Комп’ютерне моделювання інформаційних систем в умовах конфліктних взаємодій».

Пояснювальна записка містить вступ, 4 розділи, висновки, додатки та список літератури, включає 111 сторінок, 7 таблиць, 27 ілюстрації та 35 джерел.

У першому розділі проведений аналіз умов функціонування інформаційних систем, аналіз процесу виявлення та усунення вразливостей в інформаційних системах та аналіз використання вразливостей для організації негативних впливів на інформаційну систему, чим обгрунтовується актуальность роботи.

У другому розділі зазначається чітка мета та задачі для досягення даної мети. Також розділ включає в себе методи дослідження та вибір засобів реалізації.

У третьому розділі описується розробка математичних моделей. Зокрема математична модель функціонування інформаційних систем в умовах конфліктних взаємодій, математична модель конфлікту інформаційної системи без засобів захисту інформації та джерела негативного впливу. Моделюється, власне, процес розробки математичної та імітаційно моделей, а також представлена об'єктно-орієнтовані моделі конфліктної взаємодії.

У четвертому розділі описується розробка імітаційної моделі конфлікту інформаційної системи та джерела негативного впливу, відбувається порівняння результатів імітаційної та математичної моделей, а також проводиться моделювання інформаційної системи підприємства ТОВ «ІТЦ Ісланд-Україна».

Результатом проведеної роботи є розроблені математичні моделі функціонування інформаційних систем при наявності на них негативного впливу, а також об'єктно-орієнтовані та імітаційна модель.

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

ЗМІСТ

ВСТУП

Актуальність. Ускладнення завдань, що виконуються сучасними інформаційними системами, розвиток використовуваних у них інформаційних технологій, а також виникнення умов функціонування вимагає нових підходів до аналізу та прогнозування надійності ІС. Підходи, які використовуються, не враховують як динаміку вразливостей в інформаційних системах, так і динаміку навмисного негативного впливу на інформаційні системи або ж моделюють їх без урахування ряду важливих факторів, які проявляються саме в умовах конфліктної взаємодії.

Об’єкт. Конфліктні взаємодії в інформаційних системах.

Предмет дослідження. Модель інформаційної системи в умовах конфліктних взаємодій.

Мета. Розробка моделі і алгоритму аналізу надійності використання програмного забезпечення в інформаційних системах в умовах конфліктних взаємодій.

Гіпотеза дослідження. Якщо побудувати напівмарківську модель виялення та усунення конфліктних взаємодій та відповідну їй stateflow модель конфліктної ситуації, то можна аналізувати, а вподальшому і прогнозувати наслідки альтернативних стратегій організаційно-технічних заходів.

Наукова новизна. 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.

Практична цінність. Модель дозволяє імітувати конфліктні взаємодії інформаційних систем з джерелами негативного впливу

Публікації. За матеріалами дослідження опубліковано 6 наукових робіт.

Апробації. Результати доповідались на 6 наукових конференціях:

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

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

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

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

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

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

Впровадження. Результати впроваджено:

– у навчальний процес Сумського державного університету;

– у процес підтримки програмного комплексу ТОВ «ІТЦ Ісланд-Україна».

Копії актів впровадження наведені у додатку В.

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

– 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 Інформаційних технологій 27-28 березня 2019р.;

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

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

Копії дипломів представлені у додатку Д.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз умов функціонування інформаційних систем

Програмне забезпечення (ПЗ), яке встановлене в інформаційній системі (ІС), представляє собою операційну систему, а також різні утиліти та прикладні програми, серед яких, наприклад, засоби захисту інформації (ЗЗІ), особливістю яких є наявність малої кількості вразливостей. Дані засоби призначені та дозволяють закрити доступ до інших ПЗ в ІС при наявності в ІС конфліктних взаємодій.

Успіх негативного впливу (НВ) на ІС майже повністю визначається моментом часу, в який вразливість ПЗ використовується. Таким чином, особливо важливим стає точне визначення та дослідження життєвого циклу вразливостей [1-3]. Такий життєвий цикл описується певними подіями (або датами цих подій). У різних роботах [1-3] списки цих подій різні як за кількістю подій, так і за їх складом, але, деяких важливих подій немає ні в одному з таких списків (або вони включені в інші події). У зв'язку з цим, нижче наведений перелік подій, що визначає життєвий цикл вразливостей, який являє собою об'єднання вже існуючих списків з додаванням відсутніх подій:

– дата ін'єкції – це дата, коли цей вразливий код був вперше зареєстрований в репозиторії вихідного коду розробника. Але якщо репозиторій не використовується, то це – перша дата, коли вразливий код був доданий до збірки або ж скомпільовано;

– дата випуску – це дата загальнодоступного випуску системи, яка вперше містить певну вразливість;

– дата виявлення – це дата, коли вперше було виявлено вразливість;

– дата розкриття – це дата, коли організація або ж окрема людина, якій вдалося виявити вразливість, вперше про неї повідомила вендора (постачальника ПЗ) або спеціальні установи, що займаються розкриттям вразливостей;

– дата публікації – це дата, коли існування вразливості оголошується публічно відомим, наприклад, через загальнодоступні форуми чи випуск патча.

Дата публікації вразливості частіше всього збігається з датою випуску патча, який закриває її;

– дата випуску тимчасового рішення – це дата, коли випускається перше тимчасове рішення, що описує, яким методом та способом необхідно усунути вразливість. При чому неважливо офіційно воно випущене (від постачальника) або ж чи є воно коректним (відсутні відмови);

– дата випуску патча (оновлення ПЗ, яке закриває вразливість) – це дата, коли випускається перше виправлення для вразливості, незалежно від того, чи офіційне виправлення (від постачальника) чи коректне воно (відсутні відмови);

– дата інсталяції патча або застосування тимчасового рішення – це дата, коли на ІС був встановлений патч, який саме закриває вразливість або ж було використано тимчасове рішення, що також усуває вразливість.

– дата створення експлойта (програми або скрипта, що використовує уразливість ПЗ для НВ на ІС) – це дата, коли був випущений перший автоматизований експлойт (скрипт або програма), що використовує певну вразливість для негативного впливу на ІС.

– Відповідно, в залежності від того, чи настала уже та чи інша подія, вразливостям можна присвоїти наступні статуси:

– невідома вразливість. Невідома вразливість існує в ПЗ, але її ще не було виявлено;

– секретна вразливість. Секретну вразливість було виявлено, але той, хто її виявив, ще не повідомив про неї вендору (постачальнику ПЗ), громадськості або спеціальній установі, яка займається розкриттям вразливостей. Якщо людина, яка виявила вразливість – джерело НВ (ДНВ), то вона може бути використана для негативного впливу на ІС;

– розкрита вразливість. Розкриту вразливість було виявлено, і той, хто її виявив, розкрив інформацію про неї вендору або установі, що займається розкриттям вразливостей;

– опублікована вразливість. Опубліковану вразливість було виявлено і оприлюднено або через патч або ж через загальнодоступний інтернет-ресурс (форум, сайт тощо) та через засоби масової інформації;

– уразливість, для якої існує тимчасове рішення. Уразливість, для якої існує тимчасове рішення – це вразливість, для якої було створено хоча б одне тимчасове рішення, що її закриває;

– уразливість, для якої існує патч. Уразливість, для якої існує патч – це вразливість, для якої був створений хоча б один патч, що її закриває;

– закрита вразливість. Закрита вразливість – це вразливість, що була видалена з інформаційної системи за допомогою інсталяції патча, або ж за допомогою застосування тимчасового рішення;

– уразливість, для якої існує експлойт. Уразливість, для якої існує експлойт – це вразливість, для якої був створений хоча б один експлойт (програма або скрипт, яка використовує цю вразливість);

При цьому одна вразливість може володіти декількома статусами відразу. Наприклад, вразливість може одночасно мати патч і мати експлойт. Визначальними умовами для потенційної надійності тієї чи іншої ІС є дві ключовції події в життєвому циклі уразливості – виявлення вразливості та закриття вразливості. Якщо вразливість ще не виявлена або вже закрита, то вона не може бути використана ДНВ, якщо ж вона виявлена, але ще не закрита, то, відповідно – може.

Від кількості відомих вразливостей в ІС, від швидкості їх усунення, також від швидкості їх знаходження та легкості їх використання для НВ та від наслідків використання залежить надійність цієї ІС.

Тобто, для того щоб охарактеризувати умови функціонування сучасних інформаційних систем при наявності навмисних НВ (ННВ), є необхідним описати процес того, як виявити ці уразливості, та як саме вони використовуються ДНВ для ННВ на ІС, та як вони усуваються.

1.2 Аналіз процесу виявлення та усунення вразливостей

Пошуком вразливостей в ПЗ займаються ДНВ, які використовують їх для негативних впливів на ІС розробники ПЗ, спеціальні фірми, що працюють в галузі безпеки ІС і другі зацікавлені в цьому люди та організації. Але вразливості можуть бути виявлені і випадково в процесі використання будь-якого ПЗ [3].

Швидкість виявлення нових вразливостей в ПЗ залежить як від заздалегідь визначених факторів, так і від рівня перевірки ПЗ на наявність вразливостей до його офіційного випуску, кількість рядків у програмному коді (або розмір ПЗ), але також і від чинників, що змінюються в часі: від популярності ПЗ (кількість ІС, в яких це ПЗ використовується) та від якихось випадкових факторів. З останнього випливає, що швидкість виявлення нових вразливостей залежить також від часу. Нижче наведена таблиця, де містяться середньорічні швидкості виявлення вразливостей (кількість вразливостей в місяць) в Windows XP за 10 років [4].

Таблиця 1.1 – Середньорічна шидкість вияленння вразливостей у Windows XP

Період життя ПЗ, рік	Середньорічна шидкість вияленння вразливостей, од/місяць
1	1,5
2	3,17
3	2,75
4	5,5
5	5,25
6	9,58
7	5,17
8	9,5
9	17,08
10	21,92

Щоб усунути уразливість з ІС, адміністратору ІС потрібно або деінсталювати ПЗ, який містить уразливість, або встановити патч, який створюють розробниками ПЗ, щоб закрити цю уразливість, або застосувати тимчасове будь яке рішення, що усуває можливість використання уразливості. Такі тимчасові рішення публікують розробники ПЗ, та інші учасники ІТ спільноти.

Пошук патчів, які б закривали уразливості та їх установку можуть проводитися системними адміністраторами як самостійно, а також за допомогою спеціальних програм, які автоматично знаходять оновлення ПЗ на сайтах вендорів та встановлюють їх.

Системні адміністратори можуть ще використовувати сканери вразливостей (такі ж, як і ДНВ), для пошуку вразливостей в ІС. А також адміністратори ІС можуть встановлювати спеціальне програмне забезпечення для захисту ІС. В цьому випадку ДНВ перед зломом ІС спочатку необхідно буде зламати це спеціальне ПЗ, використовуючи вразливості, які в ньому є.

Організації можуть також наймати так званих "етичних" або "білих" ДНВ для визначення слабких місць в їх ІС (в тому числі для знаходження вразливостей, які ніким до цього ще не виявлялися) та їх усунення [5].

Швидкість усунення вразливостей, з одного боку, залежить від рівня технічної підтримки ПЗ, тобто від того, як швидко вендор створює патчі та випускає тимчасові рішення, що закривають уразливості, та з іншого боку, від рівня (підготовки або виконання своїх обов'язків) системного адміністратора, тобто від того, як швидко він встановлює патчі та застосовує тимчасові рішення, які закривають уразливості, та чи може він самостійно (в тому числі і за допомогою спеціального ПО) знаходити вразливості, а також придумувати тимчасові рішення для їх закриття.

Узагальнена структурна схема суб'єктів та основних процесів, які впливають на надійність ІС та реалізованих в них інформаційних технологій (ІТ), представлена на рисунку 1.1.

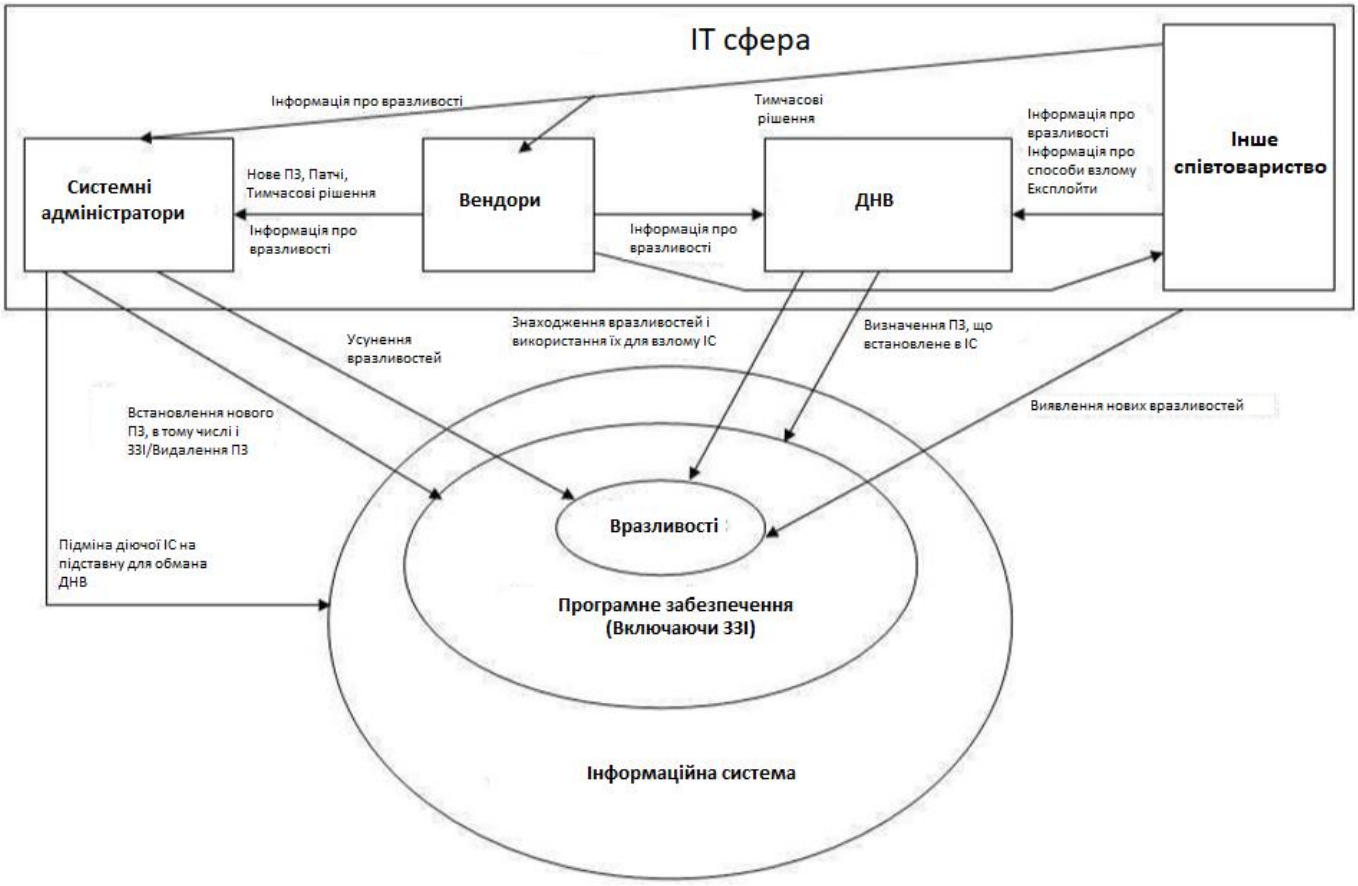


Рисунок 1.1 – Схема основних процесів, що впливають на надійність ІС

Аналіз умов функціонування сучасних інформаційних систем, схематично представлених вище, де показується, що на надійність роботи ІС впливає дуже багато факторів, причому в граничних випадках будь-який з них може виявитися визначальним.

Більшість з цих факторів мають випадковий характер, що має бути обов'язково враховано в моделях, які описують поведінку ІС при наявності ННВ.

Також зрозуміло, що умови функціонування сучасних інформаційних систем при наявності ННВ не є статичними, а вони змінюються в часі. Змінюється швидкість виявлення вразливостей, змінюється швидкість їх усунення, змінюються можливості ДНВ (а також, власне, і самі ДНВ) які негативно впливають на ІС. У зв'язку з цим статичні моделі, які описують стан сучасних ІС, будуть явно недостовірними.

Процес закриття вразливостей безпосередньо впливає на процес використання вразливостей для ННВ, а саме, моделі, що описують поведінку ІС

при наявності ННВ, повинні враховувати динаміку не тільки окремих процесів, але й динаміку конфліктної взаємодії між різними суб'єктами, які беруть участь в цих процесах.

Деякі з характеристик, що описують роботу ІС, залежать від часу, то для визначення того, наскільки надійно буде функціонувати інформаційна система при наявності НВ, потрібно визначати не поточні значення цих характеристик, а їх майбутні значення, тобто за період, для якого аналізується надійність роботи ІС, робити прогноз щодо цих характеристик.

Важливою вимогою до створюваних алгоритмів та моделей буде наявність можливості простого удосконалення таких алгоритмів і моделей, які не потребують серйозних змін в їх концепції, так як в конкретній ситуації протистояння ІС і ДНВ можуть мати місце додаткові обмеження та можливі умови реалізації конфліктної взаємодії. Крім того, розроблені алгоритми та моделі повинні використовувати параметри, для оцінки яких існують доступні джерела даних.

1.3 Аналіз використання вразливостей для організації навмисних негативних впливів на інформаційну систему

У загальному випадку реалізація навмисного НВ (ННВ) на ІС включає кілька фаз [3]. Джерелом негативного впливу може бути зловмисник або незалежний тестувальник системи, а також користувач, що здійснює помилки в процесі роботи системи і діючий в позаштатному режимі. У найбільш загальному випадку таких фаз може бути п’ять:

– розвідка: ДНВ збирає інформацію про ІС, використовуючи активні або пасивні засоби;

– сканування: ДНВ починає активно зондувати ІС для пошуку вразливостей, які можуть бути використані для ННВ;

– отримання доступу: якщо вразливість виявлена, ДНВ використовує її, щоб отримати доступ до ІС;

– підтримка доступу: як тільки доступ до ІС отримано, ДНВ зазвичай займається підтримкою доступу, щоб реалізувати мету негативного впливу;

– знищення слідів: ДНВ намагається знищити всі докази здійснення ННВ.

Не всі з п’яти наведених етапів ННВ обов'язкові, а з точки зору аналізу надійності оцінюваної ІС (тому що в 4-му і 5-му випадках ІС вже зламана) здається доречним розділити ННВ на 3 етапи [4,5]:

– визначення (інвентаризація) ПЗ, встановленого в ІС;

– визначення вразливостей в ПЗ (хоча б однієї);

– визначення способу використання уразливості для негативного впливу на ІС.

Таке уявлення ННВ дозволяє охарактеризувати ДНВ через середній час, який йому необхідно на кожен з цих етапів, при цьому ці часи будуть залежати, з одного боку, від кваліфікації ДНВ, а з іншого боку, від його рівня обізнаності про ІС. На практиці навмисно негативно впливати на ІС може не одне ДНВ, а команда ДНВ, яка може використовувати поділ праці, що також має враховуватися при аналізі надійності ІС.

Під час проведення з боку ДНВ негативного впливу, вразливість, яку він хоче використовувати, може бути закрита адміністратором ІС, внаслідок чого ДНВ не зможе завершити його. Тобто від того, з якою швидкістю будуть закриватися уразливості в ПЗ, встановленому в ІС, буде прямо залежати надійність цієї ІС.

Також можливий варіант, що ІС буде захищена за допомогою спеціальних засобів захисту інформації (ЗЗІ), типу мережевих екранів. ДНВ ПЗ відношенню до цих засобів може бути зовнішнім або внутрішнім. Під зовнішнім ДНВ в цьому випадку розуміється ДНВ, якому для успішного негативного впливу на ІС спочатку потрібно негативно вплинути на ЗЗІ, тим самим подолавши захист, а потім вже на саму ІС, використовуючи вразливості в її ПЗ. Під внутрішнім ДНВ

розуміється ДНВ, який відразу і безпосередньо може негативно впливати на ІС, використовуючи вразливості в її ПО. Можливий і варіант, коли використовується обман ДНВ, і замість реальної ІС підставляється несправжня, фіктивна. І ДНВ досліджують її до тих пір, поки не розкриють обман. Усі ці можливості повинні бути враховані при створенні моделей і алгоритмів аналізу надійності використання ПЗ в ІС в умовах ННВ.

2 ПОСТАНОВКА ЗАДАЧІ

2.1 Мета та задачі

Метою даної роботи є розробка моделей і алгоритмів аналізу та прогнозування надійності використання програмного забезпечення в інформаційних системах в умовах конфліктних взаємодій.

У ході виконання проекту необхідно створити математичну модель, яка забезпечить представлення процесу появи і усунення вразливостей як напівмарківського процесу і буде опиратись не лише на поточний стан інформаційної системи, але й дозволить передбачити її надійність у майбутньому. Також необхідно розробити об'єктно-орієнтовані моделі інформаційної системи в динаміці конфліктної взаємодії, імітаційні моделі використання динаміки конфліктної взаємодії.

Для виконання даної роботи необхідно вирішити наступні задачі:

– аналіз найбільш важливих факторів, що впливають на надійність використання ПЗ в ІС;

– визначення основних вимог до розроблюваних алгоритмів і моделей аналізу надійності використання ПЗ в ІС в умовах конфліктних взаємодій;

– аналіз сучасних підходів до оцінки надійності використання ПЗ в ІС на предмет врахування даних факторів і вимог;

– розробка моделей функціонування інформаційних систем при наявності внутрішніх вразливостей;

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

2.2 Методи дослідження

На даний момент існує велика кількість підходів до аналізу надійності в умовах негативних впливів як в цілому ІС, так і окремих інформаційних технологій [6-8]. На відміну від відомих робіт [6-8], присвячених оцінці впливу на надійність будь-яких дефектів ПЗ, в даній роботі основна увага приділена аналізу підходів [6-9], які так чи інакше зачіпають питання можливості використання вразливостей ПЗ для зовнішніх негативних впливів, що порушують працездатність ІС.

Ці підходи можна розділити на 3 категорії:

– підходи, офіційно закріплені нормативними документами, що мають державний або міжнародний статус.

– підходи, які використовуються на ринку послуг комп'ютерної безпеки (в бізнесі).

– підходи, що мають на даний момент тільки науковий додаток.

При порівнянні різних підходів необхідно звертати увагу на те, наскільки повно вони враховують реальні умови функціонування ІС при наявності ННВ: скільки факторів вони враховують, які це чинники і яким чином вони враховуються.

Виходячи з вищесказаного, підходи до аналізу надійності інформаційних систем при ННВ, слід порівнювати за наступними критеріями:

– Чи враховується динаміка надійності ІС (тобто фактично, враховуються процеси чи враховуються конкретні стани ІС).

– Які процеси враховуються.

– Чи враховується недетермінований характер процесів.

– Які параметри, від яких залежать процеси, враховуються.

– Як оцінюються параметри, що враховуються (оцінка на основі наявної статистики, оцінка на основі прогнозу).

Порівнюючи підходи до аналізу надійності ІС при цілеспрямованих негативних впливах ПЗ 1 критерію, їх можна розділити на 2 категорії:

– статичні підходи;

– динамічні підходи.

До 1 категорії статичних підходів відносяться такі, що враховують тільки конкретний стан ІС, в основному це поточний стан. Тобто аналізуються поточні умови функціонування ІС, і на основі цього аналізу робиться оцінка про надійність ІС. При цьому передбачається, що поточні умови функціонування ІС мінятися не будуть, а якщо вони все-таки будуть змінюватися, то ці зміни будуть санкціоновані адміністраторами ІС, внаслідок чого вони зможуть при таких змінах оперативно оцінити надійність ІС в нових умовах. Головна проблема такого підходу полягає в тому, що далеко не всі зміни в умовах функціонування ІС залежать від її адміністраторів. Надійність ІС залежить від 3 процесів: від виявлення вразливостей в ПЗ, від використання цих вразливостей ДНВ для ННВ на ІС і від закриття вразливостей, а також від динаміки конфліктної взаємодії між процесами закриття вразливостей і процесом ННВ на ІС. Адміністратори ІС можуть впливати тільки на процес закриття вразливостей, і то для установки патча або застосування тимчасового рішення, який закриває вразливість, адміністраторам необхідно мати в наявності цей патч або тимчасове рішення, а їх наявність майже цілком і повністю залежить від вендора, що випускає ПЗ, в якому була знайдена вразливість (хоча, звичайно, якщо адміністратор ІС володіє дуже високою кваліфікацією, він і сам може розробити тимчасове рішення, що усуває вразливість).

Тобто, ПЗ суті, статичні підходи мають наступні недоліки:

– не враховують динаміку процесів виявлення і закриття вразливостей в ІС;

– не враховують динаміку ННВ на ІС;

– не враховують динаміку конфлікту між системним адміністратором, що закриває вразливості, і ДНВ, які намагаються здійснити ННВ на ІС.

Динамічні підходи [6,10-11], на відміну від статичних, розглядають показники, що характеризують процеси, що впливають на надійність ІС, а не показники, що характеризують конкретні стани ІС. Як приклад можна привести модель, що описує динаміку появи вразливостей в ІС, засновану на теорії масового обслуговування [6], модель конфлікту ДНВ і ІС [10] і модель оцінки надійності системи захисту інформації від несанкціонованого доступу [11]. Розглянемо детальніше.

Модель, що описує динаміку появи вразливостей в ІС, заснована на теорії масового обслуговування. В [29] пропонується уявити процес появи нових вразливостей і їх усунення у вигляді роботи системи масового обслуговування (ЗМО), на вхід якої надходить пуассоновский потік заявок (вразливостей) з інтенсивністю λ, і далі ЗМО обслуговує ці заявки (усуває уразливості) з інтенсивністю μ . Крім того, передбачається, що робота над усуненням кожну уразливість починається відразу ж після її виявлення, відповідно, даний ЗМО має нескінченне число каналів обслуговування. В даних припущеннях ймовірність того, що в системі відсутні уразливості, вийшла рівною [29]:

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

Можна показати, що з урахуванням формули [59]:

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

вираз (2.1) приймає вид:

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

Дані для оцінки параметрів моделі [29] інтенсивності відкриття вразливостей λ і інтенсивності закриття вразливостей μ пропонується брати з поточної статистики [29]. Отже, підхід, запропонований в [29], не враховує, що параметри процесів виявлення і закриття вразливостей з часом змінюються, і для найбільш точного аналізу надійності ІС необхідно здійснювати прогноз для цих параметрів на період оцінки. Крім того, даний підхід не враховує залежність надійності ІС від характеристик ДНВ, які можуть здійснювати негативні впливи на цю ІС (в тому числі кількість ДНВ і розподіл праці між ними).

Модель конфлікту ДНВ і ІС, запропонована в [10], являє собою випадковий напівмарковський процес (рис. 1.2), побудований на основі концептуальної моделі конфлікту ІС – ДНВ(рис. 1.3)

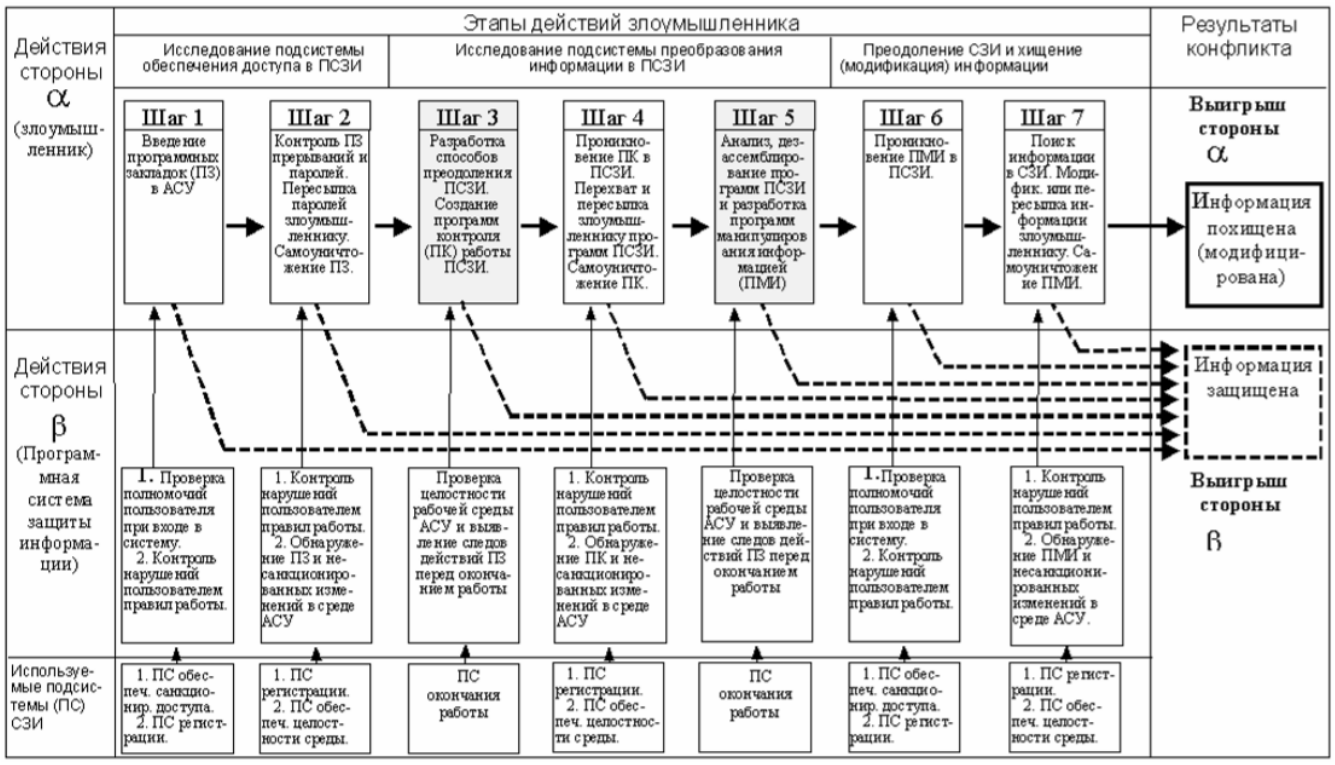


Рисунок 2.1 – Концептуальна модель конфлікту ІС – ДНВ [10]

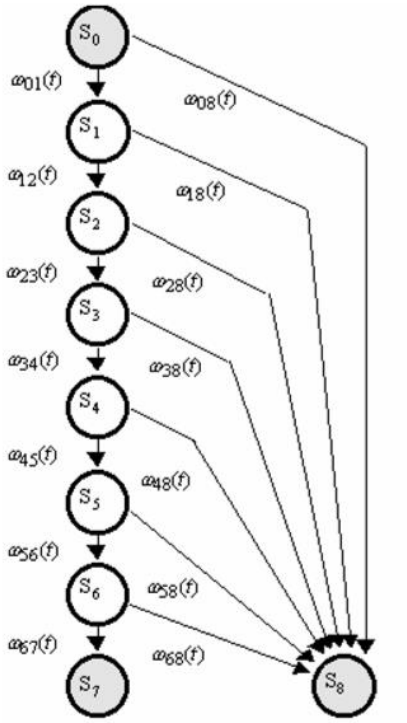


Рисунок 2.2 – Напівмарківський процес, що описує конфлікт ДНВ і ІС [10]

Стани даного процесу відображають етапи цілеспрямованого негативного впливу ДНВ на ІС [10]:

S_0 – початковий стан процесу;

S_7 – кінцевий стан процесу, відповідає виграшу сторони α (інформація модифікована ДНВ);

S_8 – кінцевий стан процесу, відповідає виграшу стороні β (інформація захищена);

S_1, S_2 … S_6 – проміжні стани процесу, відповідають успішному виконанню ДНВ відповідних кроків щодо доступу до інформації. Переходи між станами характеризуються густиною ймовірності $\omega_{01}(t), \omega_{12}(t), \omega_{23}(t), \omega_{34}(t), \omega_{45}(t), \omega_{56}(t), \omega_{67}(t), \omega_{08}(t), \omega_{18}(t), \omega_{28}(t),$

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

Далі в [10] показано, що вирішуючи систему рівнянь для випадкового напівмарковських процесу, можна визначити ймовірності виграшу сторін α та β, які будуть відповідати можливостям того, що ДНВ модифікує інформацію, або ж не зможе цього зробити.

На відміну від попереднього описаного динамічного підходу до аналізу надійності інформаційних систем в умовах внутрішніх вразливостей і навмисних негативних впливів, даний підхід дозволяє врахувати характеристики ДНВ, які можуть негативно впливати на ІС, але при цьому не враховує залежність можливості навмисного негативного впливу на ІС від наявності вразливостей і відповідно динаміку вразливостей в ІС. Крім того, видається недоцільним вибір даних етапів навмисного негативного впливу. Експерти в області комп'ютерної безпеки і самі ДНВ поділяють процес навмисного негативного впливу іншим чином, описаним в [12], тому статистику, за допомогою якої можна було б оцінити щільності ймовірності переходів між станами процесу конфлікту ДНВ і ІС, описаного в [10], неможливо де-небудь знайти або ж отримати самостійно. І, нарешті, даний підхід не враховує ні атаки на відмову в обслуговуванні, ні можливості відновлення ІС після того, як ДНВ модифікує інформацію (наприклад, інформацію можна відновити з резервної копії, що зберігається в інший ІС).

Обидва описанних вище динамічних підходи до аналізу надійнсті ІС припускають, що процеси, які впливають на надійність ІС – випадкові, що, безумовно, поряд з введенням динамічних характеристик умов функціонування ІС, є їх перевагою перед статичними підходами. Проте, не дивлячись на очевидні переваги, динамічні підходи на даний момент мають в основному тільки дослідний додаток. Нижче наведена таблиця порівняння описаних статичних і динамічних підходів.

Таблиця 2.1 – Порівняння статичних та динамічних підходів

Фактори \ Підходи		Методика ФСТЕК	CRAMM	FRAP	OCTAVE	Модель динаміки вразливостей в ІС	Модель конфлікту у ДНВ та ІС
ІС	ПЗ	+	+	+	+	+	+
	Наявність ЗЗІ	+	+	+	+	+	+

Продовження таблиці 2.1

	Наявність засобів обману	-	-	-	-	-	-
вразливості	Залежність загроз від наявності вразливостей	+	-	-	+	+	-
	Динаміка виявлення і закриття вразливостей	-	-	-	-	+	-
	Прогноз швидкості виявлення вразливостей	-	-	-	-	-	-
обслуго-вування ІС	Рівень вендора	-	-	-	-	+	-
	Рівень системного адміністра-тора	-	-	-	-	-	+
ДНВ	Кваліфікація	-	-	-	-	+	+
	Проінформо-ваність про ІС	+/-	-	-	-	+	+
	Кількість ДНВ	-	-	-	-	-	-
	Розподіл праці	-	-	-	-	-	-
	Етапи ННВ	-	-	-	-	-	+
	Динаміка ННВ	-	-	-	-	-	+
Динаміка конфлікту ДНВ та ІС		-	-	-	-	-	+

2.3 Вибір засобів реалізації

При вирішенні поставлених у роботі завдань використовувалися апарат теорії ймовірностей і математичної статистики, моделі і методи теорії систем масового обслуговування, математичний апарат ланцюгів Маркова, а також технології комп'ютерного імітаційного моделювання.

При моделюванні інформаційних процесів і систем будуть використовуватися три типи моделей: об'єктно-орієнтовані моделі в нотаціях UML, математичні моделі, засновані на використанні тих чи інших імовірнісних описів динаміки конфлікту, і комп'ютерні моделі, реалізовані в інтегрованому середовищі Matlab + Simulink + Stateflow, що забезпечує адекватне врахування вихідних концептуальних і функціональних об'єктних уявлень.

Для розроблення плану робіт, який складається з діаграми Ганта та мережевого графіку, будуть використанні такі інструменти, як: програма GanttProject та додаток MS Visio 2016. Ці засоби є найбільш ефективними адже призначення GanttProject – професійна, безкоштовна програма для управління проектами. Дозволяє призначати і відстежувати завдання, виконавців, час. Будує діаграму Ганта. Вміє імпортувати проекти від Microsoft Project. Програма на відміну від наддорогих комерційних аналогів повністю відкрита та безкоштовна. Зручний інтерфейс, який не містить нічого зайвого.

Переваги GanttProject: простий, надійний, легко освоїти і читабельний; є добре налагоджена можливість отримати графічний файл з діаграмою Ганта; програма надає необхідний мінімум можливостей з управління проектами, а саме можливість призначати виконавців, аналізувати завантаження виконавців, відображати послідовність виконання завдань (почати після завершення і т.п. – всього чотири варіанти зв'язку завдань)[20].

Microsoft Visio 2016 – редактор діаграм для Windows і редактор векторної графіки . Є дуже зручним для побудови мережевого графіку та напівмарківскої моделі конфлікту ІС і ДНВ, адже має всі необхідні інструменти (стрілки, фігури,

написи) для якісної демонстрації. Більшість людей користується саме пакетом MS Office, а тому установка і користування не викличе труднощів. Інтерфейс інтуїтивно зрозумілий, функціонал широкий, редактор дуже зручний у використанні.

UML діаграми будуть розроблятися у середовищі Visual Studio. Дане середовище містить спеціальний набір інструментів саме для створення даних діаграм. Функціонал повністю забезпечує якісне створення та комфортну роботу з діаграмами.

Реалізація імітаційної моделі буде відбуватись у середовищі Matlab, використовуючи Simulink та Stateflow.

Matlab – це високорівнева мова і інтерактивне середовище для програмування, чисельних розрахунків і візуалізації результатів. За допомогою Matlab можна аналізувати дані, розробляти алгоритми, створювати моделі і додатки.

Simulink – це графічне середовище імітаційного моделювання, що дозволяє за допомогою блок-діаграм у вигляді направлених графів, будувати динамічні моделі, включаючи дискретні, безперервні і гібридні, нелінійні і розривні системи. Інтерактивне середовище Simulink, дозволяє використовувати вже готові бібліотеки блоків для моделювання електросилових, механічних і гідравлічних систем, а також застосовувати розвинений модельно-орієнтований підхід при розробці систем управління, засобів цифрового зв'язку і пристроїв реального часу.

Stateflow – це середовище для моделювання і симуляції комбінаторної і послідовної логіки прийняття рішень, заснованих на машинах станів і блок-схемах. Stateflow дозволяє комбінувати графічні і табличні уявлення, включаючи діаграми переходу станів, блок-схеми, таблиці переходу станів і таблиці істинності – для того, щоб змоделювати реакцію системи на події, умови в часі і зовнішні вхідні сигнали [30-32].

3 РОЗРОБКА МАТЕМАТИЧНИХ МОДЕЛЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ КОНФЛІКТНИХ ВЗАЄМОДІЙ

3.1 Моделювання процесу розробки математичної та імітаційної моделей

Функціональна модель – це опис системи за допомогою IDEF0 діаграми. Призначення функціональної моделі – описати уже існуючі бізнес-процеси використовуючи як природню, так і графічну мови. Методологія IDEF0 - це джерело графічної мови, за допомогою якої передається інформація про систему.

Суть даної методології – побудувати ієрархічну систему діаграм – одиничні описи фрагментів системи. Першим кроком необхідно провести в цілому опис системи, а також описати її взаємодію з навколишнім середовищем (контекстна діаграма). Далі необхідно провести функціональну декомпозицію. Для цього систему слід розбити на підсистеми і описати кожну підсистему окремо (діаграми декомпозиції). Потім необхідно розбити підсистеми на дрібніші і продовжувати таким чином до досягнення потрібного ступеню подробиць.

Кожна IDEF0-діаграма складається з блоків та дуг. Блоки необхідні для зображення функцій системи, яка моделюється, а за допомогою дуг блоки зв'язуються разом, а також таким чином відображаються взаємозв'язки та взаємодії між ними.

Функціональні блоки (дії) на діаграмах зображуються як прямокутники, які пояснюють вказані процеси, завдання або функції, які відбуваються протягом певного часу та мають розпізнавані результати. Назва роботи має бути сформована за допомогою дієслівного іменника, який означає дію [33].

Дана діаграма містить чотири блоки, так як IDEF0 вимагає, щоб діаграма містила не менше трьох, але при цьому не більше шести блоків. Дані обмеження підтримують складність діаграм та моделі на рівні, доступному для читання, розуміння та використання.

У даній діаграмі, блоки розміщені за ступенем важливості. Дане розмыщення, що має відносний порядок є домінуванням. Під домінуванням будемо розуміти те, як один блок впливає на інші блоки діаграми.

Найдомінуючішим блоком діаграми є перший з необхідної послідовності функцій. У даній схемі найбільш домінуючий блок розміщений у верхньому лівому кутку діаграми, а найменш домінуючий – у правому кутку.

На рисунку 3.1 наведена контекстна діаграма, яка показує навколишню взаємодію з процесом, а також короткий опис предметної області, мети та точки зору. Для того, щоб розпочати даний процес, необхідно мати чітку мету, що ми і як ми маємо отримати на виході, а також проаналізовані існуючі моделі, що дасть змогу на їх базі моделювати нові математичні та об’єктно-орієнтовані моделі.

Контролювати даний процес буде керівник, а також все має бути виконано згідно з технічним завдання, що було розроблено раніше. На виході мають бути наступні результати:

– математична модель конфлікту інформаційної системи без засобів захисту інформації і джерела негативного впливу;

– об'єктно-орієнтовані моделі конфліктної взаємодії;

– імітаційна модель конфлікту інформаційної системи і джерела негативного впливу.

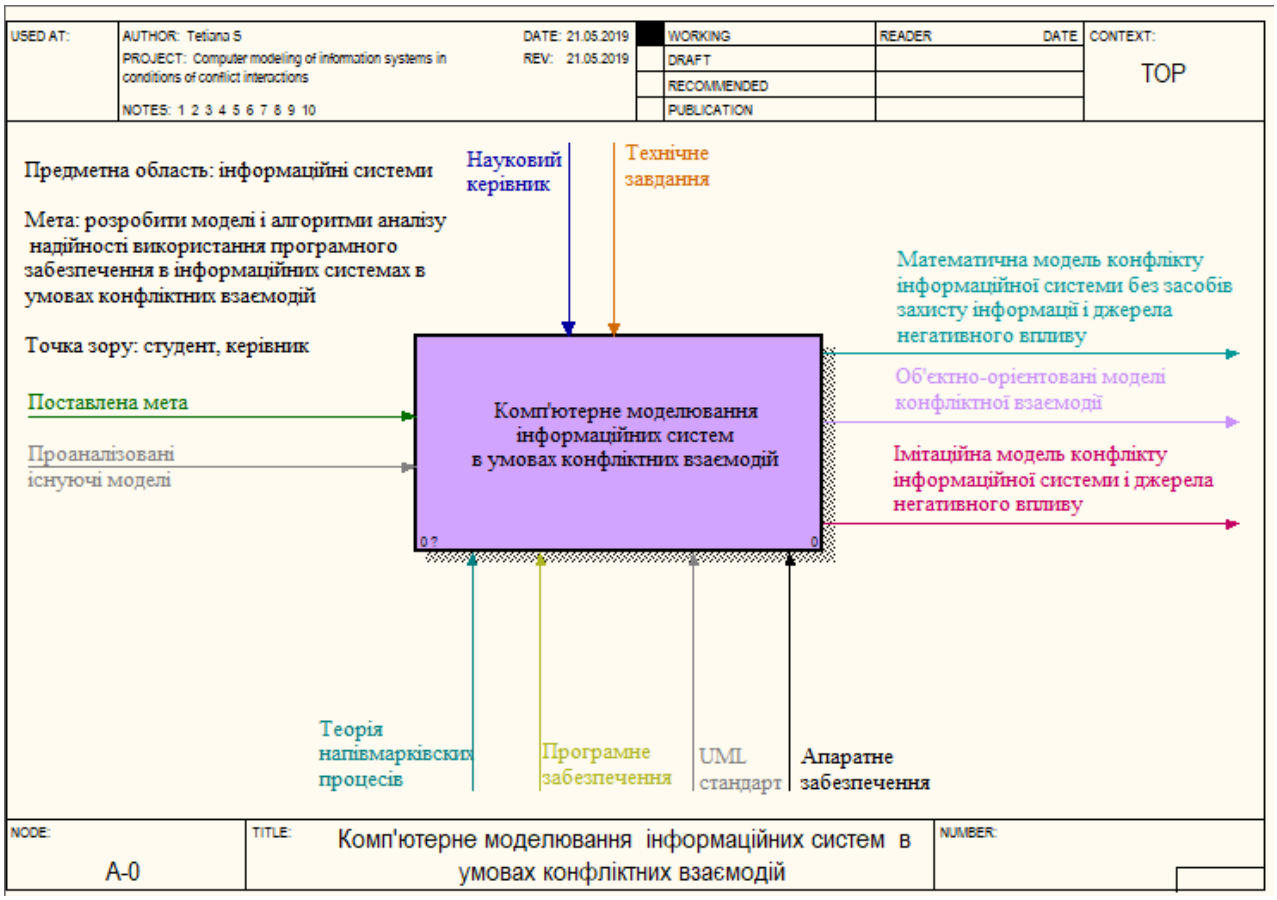


Рисунок 3.1 – Контекстна діаграма IDEF0

Дану діаграму було декомпозовано на рівень. Для того, щоб процес був виконаний, нам необідно: розробити математичну модель конфлікту інформаційної системи без засобів захисту інформації і джерела негативного впливу. Під контролем керівника та згідно з технічним завданням, використовуючи програмне та апаратне забезпечення, а також за правилами теорії напівмарківських процесів досягаємо результатів даного процесу. Після даної дії ми отримаємо математичну модель і на її основі можемо проектувати об’єктно-орієнтовані моделі, які дозволять приступити до створення імітаційної моделі. Для забезпечення . Якщо ж виникає проблема у проектуванні імітаційної моделі, є сенс перевірити об’єктно-орієнтовані моделі. Після імітаційної моделі є важливим перевірити отримані результати, а саме порівнявши математичні та дані, отримані за допомогою імітаційної моделі. Декомпозована діаграма з усіма вище описаними діями зображена на рисунку 3.2.

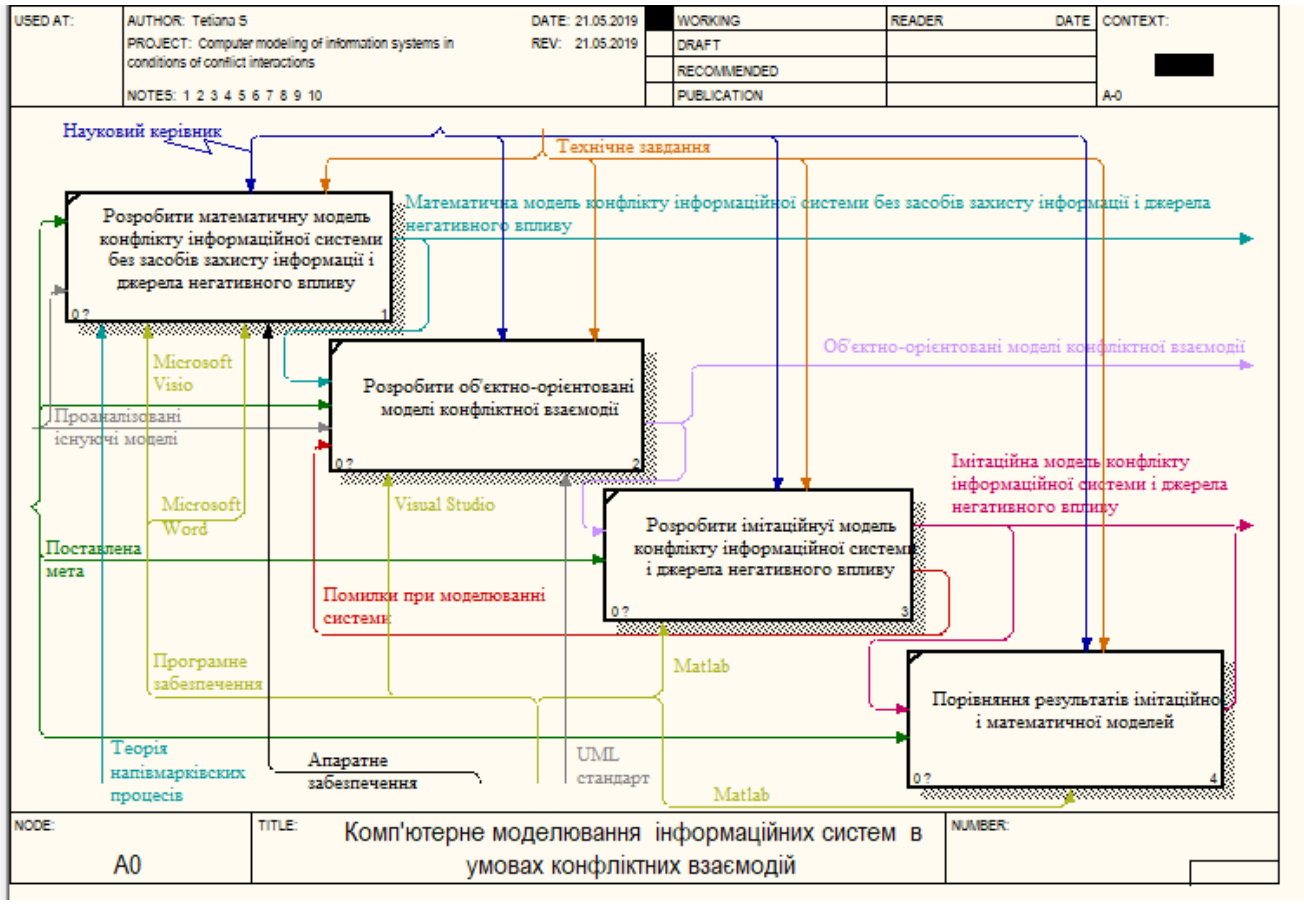


Рисунок 3.2 – Декомпозована діаграма IDEF0

Це дозволило наглядно бачити послідовність та важливість виконання дій, їх результати, а також визначити необхідне обладнання та елементи контролю.

3.2 Математична модель функціонування інформаційних систем в умовах внутрішніх вразливостей і конфліктних взаємодій

Оскільки в ІС може бути встановлено кілька різних програм, то найпростіша математична модель функціонування ІС в умовах внутрішніх вразливостей і конфліктних взаємодій може бути представлена як сукупність систем масового обслуговування, кожна з яких моделює динаміку вразливостей в кожній окремій програмі. Дана модель відображена на рисунку 2.1. Тут $\lambda^{(m)}$ – швидкість виявлення вразливостей в m-й програмі, $k^{(m)}$ – коефіцієнт, що характеризує обслуговування системним адміністратором m-ї програми, $\mathrm{T_в}^{(m)}$ – середній час створення вендором патча, який закриває вразливість, після її виявлення в m-й програмі, а M – загальна кількість програм.

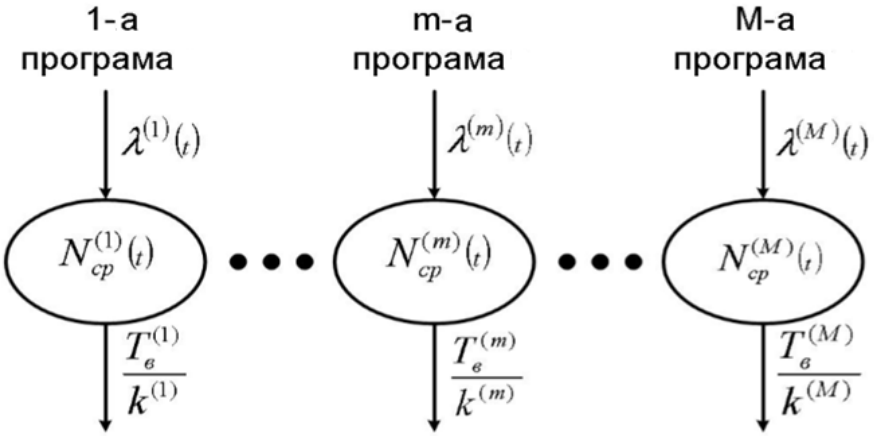


Рисунок 3.3 – Математична модель функціонування ІС (без ЗЗІ)

В цьому випадку середньостатистичне число вразливостей в ІС буде сумою середньостатистичного числа вразливостей в кожній програмі, встановленої в ІС.

$$N_{\text{ср}}(t) = \sum_{m=1}^{M} N_{\text{ср}}^{(m)}, N_{\text{ср}}^{(m)}(t) = \frac{T_{\text{в}}^{(m)} e^{-1}}{k^{(m)}} \left(\lambda^{(m)}(t) + \int_0^t \lambda^{(m)}(\tau) e^{\tau} d\tau \right) \quad (3.1)$$

Ймовірність відсутності в ІС вразливостей може бути розрахована за формулою (2.1), якщо замість середнього числа вразливостей в конкретній програмі в неї підставити середнє число вразливостей в ІС.

У найпростішому випадку, коли ДНВ має доступ до всіх програм, встановлених в ІС, і уразливості кожної програми можуть бути використані безпосередньо для негативного впливу на ІС, потенційна ймовірність того, що надійність даної ІС в момент часу t не може бути порушена ДНВ (далі ймовірність надійності ІС), збігається з ймовірністю відсутності в ІС вразливостей (в даному випадку не має значення, чи є ДНВ зовнішнім або внутрішнім).

$$P_{\text{над}}(t) = P_0(t) \quad (3.2)$$

Дана ймовірність має потенційний характер, так як при її розрахунку не враховуються характеристики ДНВ, які можуть негативно впливати на ІС, а розглядається лише потенційна можливість такого впливу. Варто відзначити, що дана ймовірність визначає не тільки можливість навмисного негативного впливу, а й можливість ненавмисного негативного впливу, наприклад, з боку шкідливого ПЗ.

3.3 Математична модель конфлікту інформаційної системи без засобів захисту інформації і джерела негативного впливу

Математична модель конфлікту грунтується на поданні процесу зміни станів об'єднаної системи ІС – ДНВ у вигляді ланцюга Маркова з кінцевим числом станів, переходи між якими здійснюються за експоненціальним (пуассонівського) закону розподілу [13]. Дана модель є розширенням найпростішої математичної моделі ІС, запропонованої вище, в плані обліку дій

ДНВ в залежності від його обізнаності та кваліфікації. На рисунку 3.4 представлені стани, в яких може перебувати ДНВ при підготовці і проведенні НВ на ІС, а також можливі переходи з одного стану в інший.

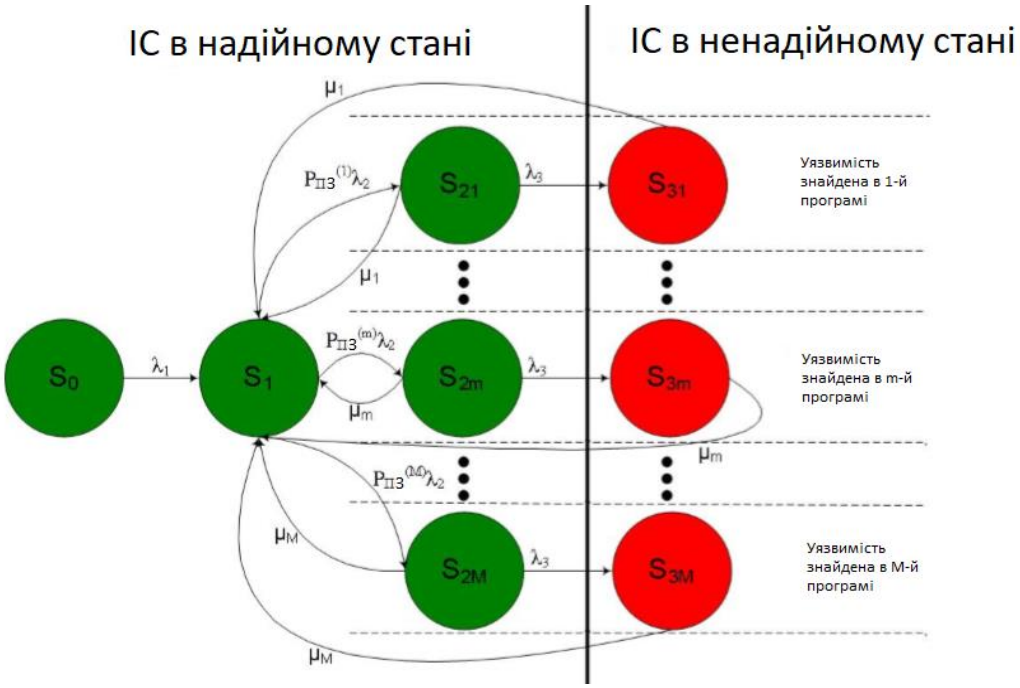


Рисунок 3.4 – Математична модель конфлікту ІС без ЗЗІ і ДНВ

Вузли ланцюга відповідають наступним станам:

S_0 – у ДНВ відсутня будь-яка інформація про ІС (стан «Немає інформації про ІС» в об'єктно-орієнтованій моделі);

S_1 – у ДНВ є інформація про ПЗ ІС (стан «Інформація про ПЗ ІС» в об'єктно-орієнтованої моделі);

S_{2m} – у ДНВ є інформація про ПЗ ІС і про одну уразливість в цьому ПО, де m – номер програми, в якій була знайдена уразливість ($m \in 1..M$), а M – кількість програм в ІС (стан «Інформація про уразливості в ПЗ ІС» в об'єктно моделі);

S_{3m} ($m \in 1..M$) – у ДНВ є інформація про ПЗ ІС, про одну вразливість в цьому ПО, а також про спосіб використання цієї вразливості для здійснення НВ на ІС (стан «Інформація про спосіб використання уразливості для НВ на ІС» в об'єктно-орієнтованої моделі).

Ймовірності знаходження в зазначених станах позначимо відповідно P_0,P_1,P_{21},…P_{2m},…P_{2M},…,P_{31},…P_{3m},….P_{3M}. При цьому частина виділених станів агрегуються в стан «ІС в надійному стані» (стан «Надійний стан» в об'єктно-орієнтованій моделі), а стани (S_{31},…S_{3m},…S_{3M}) – в стан «ІС в ненадійному стані» (стан «Ненадійний стан» в об'єктно- орієнтованій моделі).

Перехід зі стану S_0 в S_1 здійснюється з інтенсивністю:

$$\lambda_1 = \frac{1}{T_{no}}, \tag{3.3}$$

де T_{no} – середній час, потрібний ДНВ для знаходження інформації про ПЗ ІС.

Переходи зі стану S_1 в стани S_{2m} $(m \in 1..M)$ здійснюються з інтенсивностями $P_{\text{ПЗ}}^{(m)}\lambda_2$, де $P_{\text{ПЗ}}^{(m)}$- ймовірність знаходження інформації про уразливість в m-й програмі, яка дорівнює:

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

де $N_{\text{ср\_конф}}^{(m)}$ – середньоарифметичне середньостатистичного числа вразливостей, які перебувають в m-й програмі ІС $N_{\text{ср}}^{(m)}(t)$, а $N_{\text{ср\_конф}}$ – середнє арифметичне середньостатистичного загального числа вразливостей, що знаходяться в ПЗ ІС $N_{\text{ср}}(t)$.

Інтенсивність виявлення вразливостей в ПЗ ІС:

$$\lambda_2 = \frac{N_{\text{ср\_конф}}}{T_{\text{уязв}}} \tag{3.5}$$

де $T_{\text{уязв}}$ – середній час, потрібний ДНВ для знаходження інформації про всі слабкі місця в ІС. З урахуванням (3.4) і (3.5) інтенсивності переходів зі стану S_1 в стани S_{2m} $(m \in 1..M)$ будуть дорівнювати:

$$P_{\text{ПЗ}}^{(m)}\lambda_2 = \frac{N_{\text{ср\_конф}}^{(m)}}{T_{\text{уязв}}} \tag{3.6}$$

Перехід зі стану $S_{2m}(m \in 1..M)$ в стан S_{3m} $(m \in 1..M)$ здійснюються з інтенсивністю:

$$\lambda_3 = \frac{1}{T_{\text{нв}}}, \tag{3.7}$$

де $T_{\text{нв}}$ – середній час,потрібний ДНВ для знаходження інформації про спосіб використання вразливості в ПЗ ІС для НВ на ІС.

Для розрахунку середнього часу, з моменту знаходження ДНВ вразливості до її усунення з ІС, пропонується вдатися до наступних міркувань. Передбачається, що час виявлення (появи) уразливості в m-й програмі) $T_{\text{обн\_уязв}}^{(m)}$ є випадковою величиною, що приймає з однаковою ймовірністю значення з інтервалу від різниці поточного часу $T_{\text{тек}}$ і середнього часу життя вразливості в m-й програмі $T_{\text{жизн\_уязв}}^{(m)}$ до поточного часу $T_{\text{тек}}$, отже, її математичне сподівання дорівнює $T_{\text{тек}} = \frac{T_{\text{жизн\_уязв}}^{(m)}}{2}$, а час з моменту знаходження ДНВ інформації про вразливості в m-й програмі до закриття $T_{\text{закр}}^{(m)}$ цієї вразливості відповідно дорівнює:

$$T_{\text{закр}}^{(m)} = \frac{T_{\text{жизн\_уязв}}^{(m)}}{2} \tag{3.8}$$

Середній час життя уразливості в m-й програмі розраховується за формулою:

$$T_{\text{жизн\_уязв}}^{(m)} = \frac{\text{Т}_{\text{в}}^{(m)}}{k^{(m)}}, \quad (3.9)$$

де $\text{Т}_{\text{в}}^{(m)}$ – час, який потрібен вендору m-ї програми для створення патча або тимчасового рішення, що закривають вразливість, з моменту її виявлення, $k^{(m)}$ – коефіцієнт, що відображає роботу системного адміністратора щодо усунення вразливостей з m-ї програми.

Переходи зі станів $S_{2m}(m \in 1..M)$ в $S_{3m}(m \in 1..M)$ здійснюється з інтенсивностями:

$$\mu_m = \frac{1}{T_{\text{закр}}^{(m)}}, \quad (3.10)$$

Які з врахуванням 3.8 і 3.9 рівні:

$$\mu_m = \frac{2k^{(m)}}{T_{\text{в}}^{(m)}}, \quad (3.11)$$

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

$$P(0) = [1\ 0\ \ldots\ 0], \quad (3.12)$$

і перехідною матрицею:

$$P_{пер}(t) = \exp(Qt),$$

$$Q = \begin{bmatrix} 1-\lambda_1 & \lambda_1 & 0 & \dots & 0 & 0 & .. & 0 \\ 0 & 1-\sum_{m=1}^{M} P_{ПО}^{(m)}\lambda_2 & P_{ПО}^{(1)}\lambda_2 & \dots & P_{ПО}^{(M)}\lambda_2 & 0 & \dots & 0 \\ 0 & \mu_1 & 1-(\mu_1+\lambda_3) & \dots & 0 & \lambda_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \mu_M & 0 & \dots & 1-(\mu_M+\lambda_3) & 0 & \dots & \lambda_3 \\ 0 & \mu_1 & 0 & \dots & 0 & 1-\mu_1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \mu_M & 0 & \dots & 0 & 0 & .. & 1-\mu_M \end{bmatrix}, \quad (3.13)$$

де Q – матриця інтенсивностей переходів між станами ланцюга; t – поточний час, що відраховується від початку конфлікту. З урахуванням (3.3), (3.6), (3.7) і (3.9) дана перехідна матриця набуває вигляду:

$$P_{пер}(t) = \exp(Qt),$$

$$Q = \begin{bmatrix} 1-\frac{1}{T_{по}} & \frac{1}{T_{по}} & 0 & \dots & 0 & 0 & .. & 0 \\ 0 & 1-\sum_{m=1}^{M}\frac{N_{ср\_конф}^{(m)}}{T_{уязв}} & \frac{N_{ср\_конф}^{(1)}}{T_{уязв}} & \dots & \frac{N_{ср\_конф}^{(M)}}{T_{уязв}} & 0 & \dots & 0 \\ 0 & \frac{2k^{(1)}}{T_в^{(1)}} & 1-\left(\frac{2k^{(1)}}{T_в^{(1)}}+\frac{1}{T_{нв}}\right) & \dots & 0 & \frac{1}{T_{нв}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_в^{(M)}} & 0 & \dots & 1-\left(\frac{2k^{(M)}}{T_в^{(M)}}+\frac{1}{T_{нв}}\right) & 0 & \dots & \frac{1}{T_{нв}} \\ 0 & \frac{2k^{(1)}}{T_в^{(1)}} & 0 & \dots & 0 & 1-\frac{2k^{(1)}}{T_в^{(1)}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_в^{(M)}} & 0 & \dots & 0 & 0 & .. & 1-\frac{2k^{(M)}}{T_в^{(M)}} \end{bmatrix}. \quad (3.14)$$

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

$$P(t) = P(0)P_{\text{пер}}(t), \quad (3.15)$$

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

$$P_{\text{нах\_над}}\ (t) = 1 - \sum_{m=1}^{M} P_{3m}(t) \tag{3.16}$$

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

$$P_{нах\_над\_конф} = \frac{\int_0^{T_{конф}} P_{нах\_над}(t)dt}{T_{конф}}, \tag{3.17}$$

де $T_{конф}$ – час тривалості конфлікту. З урахуванням (3.15-3.16) формула (3.17) приймає вигляд:

$$P_{нах\_над\_конф} = \frac{\int_0^{T_{конф}} \left(1 - \sum_{m=1}^{M} \left(P(0)P_{пер}(t)\right)_{3m}\right)dt}{T_{конф}}. \tag{3.18}$$

Для знаходження ймовірності надійності ІС слід спростити математичну модель, прибравши переходи з станів S_{3m} ($m \in 1..M$) в стан S_1, зробивши таким чином стан S_{3m} ($m \in 1..M$) поглинаючим. Отриманий таким чином ланцюг Маркова представлений на рисунку 3.5.

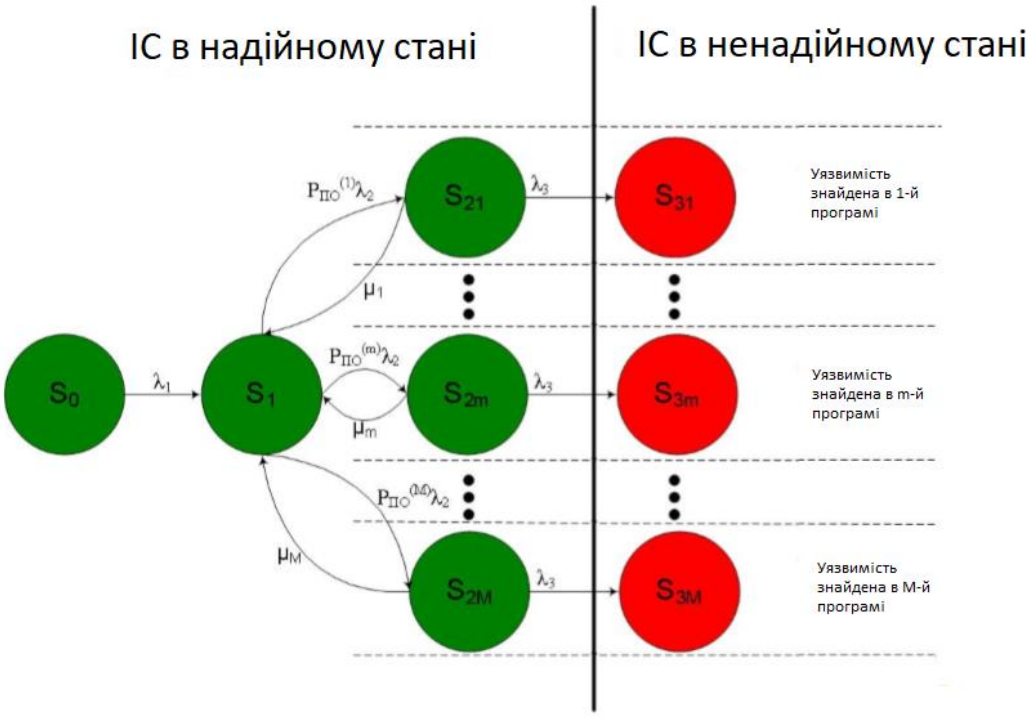


Рисунок 3.5 – Спрощена математична модель конфлікту ІС- ДНВ

Вектор початкового розподілу вірогідностей знаходження в різних станах залишається колишнім $P(0) = [1\ 0\ ...\ 0]$, а перехідна матриця має вид:

$$P_{пер}(t) = \exp(Qt),$$

$$Q = \begin{bmatrix} 1-\frac{1}{T_{по}} & \frac{1}{T_{по}} & 0 & \dots & 0 & 0 & .. & 0 \\ 0 & 1-\sum_{m=1}^{M}\frac{N_{ср\_конф}^{(m)}}{T_{уязв}} & \frac{N_{ср\_конф}^{(1)}}{T_{уязв}} & \dots & \frac{N_{ср\_конф}^{(M)}}{T_{уязв}} & 0 & \dots & 0 \\ 0 & \frac{2k^{(1)}}{T_в^{(1)}} & 1-\left(\frac{2k^{(1)}}{T_в^{(1)}}+\frac{1}{T_{нв}}\right) & \dots & 0 & \frac{1}{T_{нв}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_в^{(M)}} & 0 & \dots & 1-\left(\frac{2k^{(M)}}{T_в^{(M)}}+\frac{1}{T_{нв}}\right) & 0 & \dots & \frac{1}{T_{нв}} \\ 0 & 0 & 0 & \dots & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & .. & 1 \end{bmatrix}. \quad (3.19)$$

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

$$P_{\text{ненад}} = \sum_{m=1}^{\text{M}} P_{\text{З}m}(T_{\text{конф}}), \quad (3.20)$$

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

$$P_{\text{над}} = 1 - \sum_{m=1}^{\text{M}} P_{\text{З}m}\left(T_{\text{конф}}\right), \quad (3.21)$$

а з врахуванням 3.17:

$$P_{\text{над}} = 1 - \sum_{m=1}^{\text{M}} (P(0)P_{\text{пер}}\left(T_{\text{конф}}\right))_{\text{З}m}. \quad (3.22)$$

3.4 Об’єктно-орієнтовані моделі конфліктної взаємодії

Нехай є ІС з встановленим ПЗ. ДНВ, що навмисно впливає на ІС, як правило, проводить попередній аналіз (комп'ютерну розвідку) ПЗ, встановленого на ІС, досліджує вразливості в цьому програмному забезпеченні і можливі способи використання цих вразливостей [12]. При цьому ДНВ може мати різну кваліфікацію і можливості. Кваліфікацію і можливості ДНВ будемо описувати середнім часом, який потрібен ДНВ [15]: для отримання інформації про ПЗ ІС; для отримання інформації про всі слабкі місця в ПЗ ІВ; для отримання інформації про використання уразливості в ПЗ ІС для організації НВ на ІС. При цьому динаміка вразливостей ПЗ ІС описується найпростішою математичною моделлю ІС розглянутою вище.

Для конструювання об'єктно-орієнтованої моделі конфлікту пропонується застосувати апарат мови UML [16], використовуючи для опису поведінки сторін, що беруть участь в конфліктній взаємодії, діаграму станів. Нижче на рисунках 3.6 – 3.8 наведені діаграми станів, які описують поведінку ІС, системного адміністратора і ДНВ відповідно.

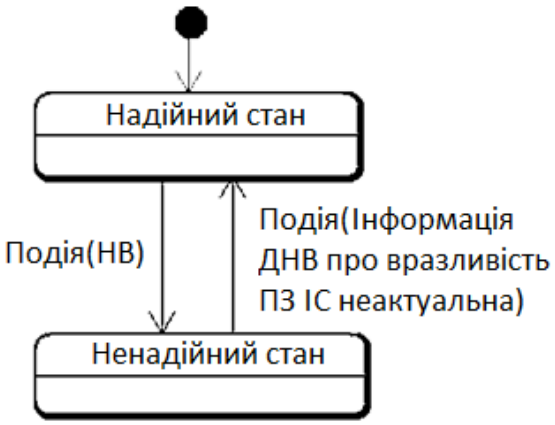


Рисунок 3.6 – Діаграма станів ІС без ЗЗІ в ході конфліктної взаємодії з ДНВ

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

– Стан «Надійний стан» – стан, при якому ДНВ не може здійснити успішний вплив на ІС.

– Стан «Ненадійний стан» – стан, при якому ДНВ може здійснити успішний вплив на ІС.

Передбачається, що ІС спочатку знаходиться в «надійному стані». Перехід з «надійного стану» в «ненадійний» здійснюється при події «НВ». Зворотний перехід здійснюється при виникненні події «Інформація ДНВ про вразливість в ПЗ ІС неактуальна».

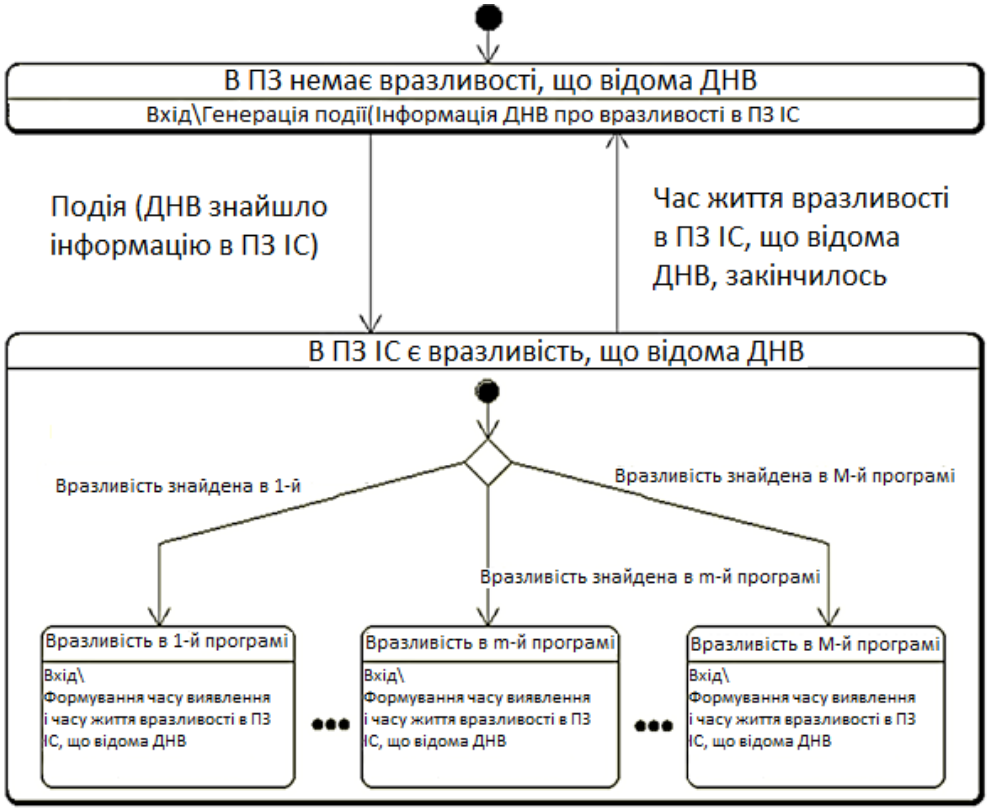


Рисунок 3.7 – Діаграма станів системного адміністратора в ході конфліктної взаємодії ІС без ЗЗІ з ДНВ

Робота системного адміністратора представляється 2-ма станами, в яких може перебувати вразливість, відома ДНВ (рис. 2.6):

– Стан «У ПЗ ІС немає вразливості, відомої ДНВ» – стан , при якому ДНВ не володіє інформацією про уразливість в ПЗ ІС ;

– Стан «У ПЗ ІС є вразливість, відома ДНВ» – стан, при якому у ДНВ є інформація про уразливість в ПЗ ІС.

Передбачається, що спочатку системний адміністратор знаходиться в першому стані («В ПЗ ІС немає уразливості, відомої ДНВ»). При вході в цей стан генерується подія «Інформація ДНВ про вразливість в ПЗ ІС неактуальна». Перехід в другий стан («В ПЗ ІС є вразливість, відома ДНВ») здійснюється при виникненні події «ДНВ знайшло інформацію про уразливість в ПЗ ІС». У другому стані відбувається вибір одного з підстанів: «Вразливість в 1-й програмі», ..., «Вразливість в 2-й програмі», ..., «Вразливість в М-й програмі» (всього в ІС встановлено М програм, $m \epsilon \overline{1,M}$) в залежності від того, в якій програмі була виявлена уразливість, в обраному підстані формується час виявлення уразливості, відомої ДНВ, і час її життя (час до створення патча або тимчасового рішення, що закриває її). Зворотний перехід зі стану «В ПЗ ІС є вразливість, відома ДНВ», в стан «В ПЗ ІС немає вразливості, відомої ДНВ», відбувається за умовою закінчення часу життя вразливості.

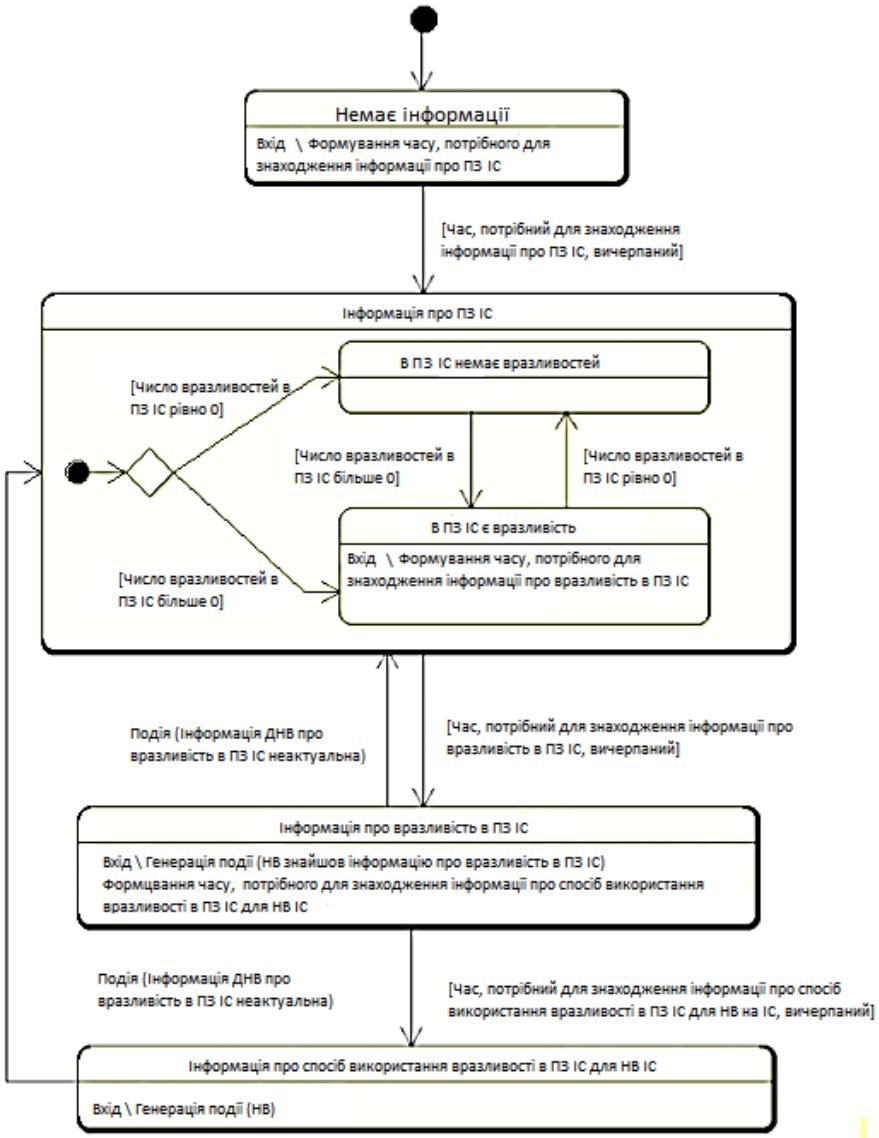


Рисунок 3.8 – Діаграма станів ДНВ в ході конфліктної взаємодії з ІС без ЗЗІ

Відповідно до рис.3.8, ДНВ може знаходиться в 4-х станах:

– Стан «Немає інформації про ІС» – початковий стан, при якому у ДНВ відсутня будь-яка інформація про ІС;

– Стан «Інформація про ПЗ ІС» – стан, при якому у ДНВ є інформація про ПЗ ІС;

– Стан «Інформація про вразливість в ПЗ ІС» – стан, при якому у ДНВ є інформація про ПЗ ІС і про одну уразливість в цьому ПО;

– Стан «Інформація про спосіб використання вразливості в ПЗ ІС для НВ на ІС» – стан, при якому у ДНВ є інформація про ПЗ ІС, про одну уразливість

в цьому ПЗ, а також інформація про спосіб використання цієї уразливості для здійснення НВ на ІС .

Передбачається, що ДНВ спочатку знаходиться в стані «Немає інформації про ІС». В даному стані формується час, необхідний НВ для знаходження інформації про ПЗ ІС. Перехід в стан «Інформація про ПЗ ІС» відбувається за умовою закінчення цього часу. Стан «Інформація про ПЗ ІС» містить 2 підстани, «В ПЗ ІС немає вразливостей» і «В ПЗ ІС є уразливості», в одне з яких ДНВ потрапляє в залежності від числа вразливостей в ІС. Якщо воно більше 0 – то в стану «В ПЗ ІС є уразливості», якщо дорівнює 0 – то в стан «В ПЗ ІС немає вразливостей». Виходячи з цього ж умови, здійснюються переходи між цими підстанів. У підстанів «В ПЗ ІС є уразливості» формується час, необхідний для знаходження однієї уразливості в ПЗ ІС. Перехід в стан «Інформація про вразливість в ПЗ ІС» відбувається ПЗ закінченню цього часу. При попаданні в даний стан генерується подія «ДНВ знайшов інформацію про вразливість в ПЗ ІС» і формується час, потрібний для знаходження інформації про спосіб використання уразливості в ПЗ ІС для НВ на ІС. Перехід в стан «Інформація про спосіб використання уразливості в ПЗ ІС для НВ на ІС» відбувається за умовою закінчення цього часу. При попаданні в даний стан генерується подія «НВ» (переводить ІС в стан «Ненадійний стан»). Також існують переходи з станів «Інформація про уразливість» і «Інформація про спосіб використання уразливості для НВ на ІС» в стан« Інформація про ПЗ ІС» в разі виникнення події« Інформація ДНВ про уразливість в ПЗ ІС неактуальна».

Таким чином, сукупність 3-х діаграм станів (рис 3.1-3.3) описує конфлікт між ІС без ЗЗІ та ДНВ, які намагаються здійснити НВ на ІС, і дозволяє на своїй основі створити математичну модель конфлікту ІС без ЗЗІ та ДНВ і імітаційну модель конфлікту ІС без ЗЗІ та ДНВ, за допомогою яких можна буде 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.

4 КОМПЮТЕРНА ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ ПРОЦЕСІВ КОНФЛІКТНИХ ВЗАЄМОДІЙ

4.1 Розробка імітаційної моделі конфлікту інформаційної системи і джерела негативного впливу

Запропонована математична модель конфлікту ІС і ДНВ враховує тільки середнє значення середньостатистичного числа вразливостей, які перебувають в ПЗ ІВ, за період конфлікту, тоді як в реальності середньостатистичне число вразливостей в ПЗ ІВ 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, ІС атакують не один, а кілька ДНВ).

Ускладнення постановки 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. 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 [17,30, 31, 32].

Вигляд моделі у середовищі Simulink продемонстровано на рисунку 3.1. У даному випадку, для проведення різних експериментів, є можливим поданням різних даних, таких як:

– t – задання імітаційного часу, що дозволить проводити імітаційні дослідження за конкретно вказаний проміжок часу;

– nuyazv – середньостатична кількість вразливостей в ІС – дані, які мають властивість змінюватися з часом, тому важливо мати змогу їх змінювати;

– nuyazv1 та nuyazv2 – середньостатична кількість вразливостей в ПЗ 1 та 2– дані, які будуть різними при імітаційному моделюванні різних ПЗ, тому є необхідність робити їх такими, що вводяться;

– T_{po} – середній час ДНВ для знаходження інформації про ПЗ;

– T_{uazv} – середній час ДНВ для знаходження інформації про всі вразливості в ІС;

– T_{nv} – середній час ДНВ для знаходження інформації про спосіб використання вразливості в ПЗ ІС;

– K – коефіцієнт адміністратора, його кваліфікація.

– T_{v1}, T_{v2}, T_{v3} – час, необхідний вендору для випуску патчу для закрится вразливості в ПЗ 1, ПЗ 2, ПЗ 3.

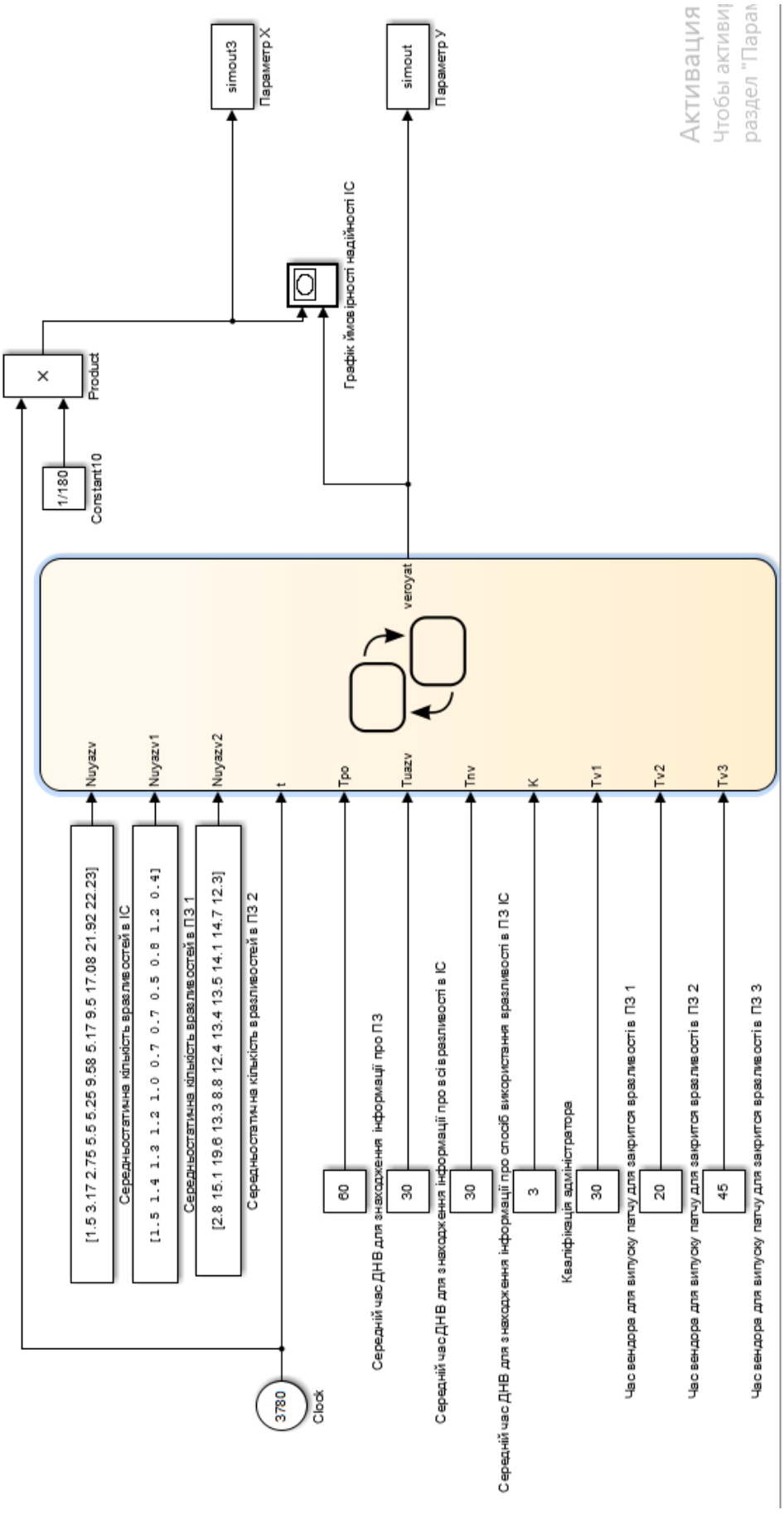


Рисунок 4.1 – Simulink модель інфрмаційної системи

Конфліктну взаємодію ІС – ДНВ в термінах [17] можна описати за допомогою SF-моделі (рис. 4.1), що грунтується на раніше представлених сукупності діаграм станів ІС, системного адміністратора і ДНВ, наведених вище (рис 3.6-3.8). Модель складається з 3-х паралельно функціонуючих об'єктів («Sysadmin» і «IS» с одного боку, «INV» з іншого боку), в яких розміщені карти станів, що описують можливі значення чинників, що враховуються і поведінку (в залежності від цих значень) всіх сторін, що беруть участь в конфлікті.

Інформаційна система (блок IS) може знаходитися в 2-х основних станах:

– Стан «Nadezhnoe sostoyanie» – стан, при якому ІС вважається захищеною від НВ ДНВ (стан «Надійний стан» в об'єктно-орієнтованій моделі).

– Стан «Nenadezhnoe sostoyanie» – стан, при якому ІС вважається незахищеною від НВ ДНВ (стан «Ненадійний стан» в об'єктно-орієнтованій моделі).

Блок «Sysadmin» імітує роботу системного адміністратора щодо усунення вразливостей, відомих ДНВ, і передбачає можливість знаходження в 2-х станах:

– Стан «Net_izv_INV_uyazv» – стан, при якому адміністратор ІС готується до закриття уразливості в ПЗ (стан «В ПЗ ІС немає уразливості, відомої ДНВ» в об'єктно-орієнтованій моделі).

– Стан «Yest_izv_INV_uyazv» – стан, при якому адміністратор ІС закриває уразливість в ПЗ, відому ІНВ (стан «В ПЗ ІС є вразливість, відома ДНВ» в об'єктно-орієнтованій моделі).

Для визначеності припустимо, що в ІС встановлено 3 види ПЗ. Тоді стан «Yest_izv_INV_uyazv» слід розбити на 3 підстани:

– «Uyazv_v_1_programme»,
– «Uyazv_v_2_programme»,
– «Uyazv_v_3_programme».

Потрапляння в один із цих станів визначається наступним чином: при вході в стан «Yest_izv_INV_uyazv» змінній Ppo присвоюється випадкова величина, рівномірно розподілена на відрізку від 0 до 1. Цей відрізок розбивається на 3

інтервали, кожен з яких відповідає виду ПЗ, в якому була виявлена уразливість. Довжина кожного інтервалу дорівнює відношенню середньостатистичного числа вразливостей в ПЗ, якому відповідає даний інтервал, до середньостатистичного числа вразливостей в ІС (у даному випадку відрізок [0,1] розбивається на інтервали [0, Nuyazv1/Nuyazv], [(Nuyazv1/Nuyazv, (Nuyazv1+Nuyazv2)/Nuyazv] та , [(Nuyazv1+Nuyazv2)/Nuyazv),1]. Якщо значення змінної Ppo потрапляє в 1-й інтервал, то блок «Sysadmin» потрапляє в підстан «Uyazv_v_1_programme», якщо у в 2-й – то в «Uyazv_v_2_programme», а якщо в 3-й – то в «Uyazv_v_3_programme». Аналогічним чином можна моделювати випадки, коли в ІС встановлено більшу або меншу кількість програм.

Попереджуючий перехід в стан «Net_izv_INV_uyazv» призводить до генерації події «net_inf_uyazv», яка переводить блок «INV» з будь-якого стану, крім «Net_informacii», в стан «Informaciya_o_PO» (інформація про уразливості та способи взлому, якими на той момент володіло ДНВ, втрачає актуальність). При цьому блок «IS» переходить в стан «Nadezhnoe sostoyanie», що відповідає переходу ІС в надійний стан.

Стани, в яких може перебувати сторона «INV», повністю відповідають станам ДНВ, визначеним у розглянутій вище об'єктно-орієнтованій моделі конфлікту ІС і ДНВ:

– Стан «Net_informacii» – початковий стан, при якому у ДНВ відсутня будь-яка інформація про систему.

– Стан «Informaciya_o_PO» – стан, при якому у ДНВ є інформація про ПЗ ІС.

– Стан «Informaciya_o_uyazvimosty» – стан, при якому у ДНВ є інформація про ПЗ ІС і про одну уразливість в цьому ПЗ.

– Стан «Invormaciya_o_sposobah_nv» – стан, при якому у ДНВ є інформація про ПЗ ІС, хоча б про одну уразливість в цьому ПЗ, а також уразливості для здійснення НВ на ІС.

Стан «Informaciya_o_PO» містить в собі 2 підстани:

– «Net_uyazv»,

– «Est_uyazv».

У підстан «Net_uyazv» блок «INV» потрапляє в разі, якщо середньостатистичне число вразливостей в ІС дорівнює 0, в підстан «Est_uyazv», якщо – більше 0. Попереджуючий перехід в стан «Informaciya_o_uyazvimosty» призводить до генерації події «inf_uyazv», яка переводить блок «Sysadmin» в стан «Yest_izv_INV_uyazv». При упереджувальному досягненні останнього стану відбувається генерація події «nv», що переводить блок «IS» в стан «Nenadezhnoe sostoyanie», що відповідає переходу ІС в ненадійний стан.

Час переходу сторони «INV» у будь-який з можливих станів описується змінною t_1. Час перебування ДНВ (сторони «INV») в станах «Net_informaci» та «Informaciya_o_uyazvimosty» у відсутності події «net_inf_uyazv» at_1 є випадковим і задається наступним чином: ml('(1/(1/%f))*log(rand)*(-1)', Tpo). Завдяки цьому формується випадкове число, розподілене за показовим законом з параметром ДНВ, що становить $1/T_{ПЗ}$, $1/T_{НВ}$ в залежності від стану. Час перебування ДНВ в стані «Informaciya_o_PO» at_{11} становить ml('(1/(1/%f))*log(rand)*(-1)', Tuazv) (відношення загального часу, потрібного ІНВ для знаходження інформації про всі слабкі місця в ПЗ ІС, до числа цих вразливостей). Переходи з одного стану в інший здійснюються за умовою закінчення часу перебування в кожному з станів.

Час життя уразливості відомої ДНВ at_2 = ml('(1/(%f/%f))*log(rand)*(-1)', K, Tv1) для першої програми, at_2 = ml('(1/(%f/%f))*log(rand)*(-1)', K, Tv2) для другої програми та відповідно at_2 = ml('(1/(%f/%f))*log(rand)*(-1)', K, Tv3) для третьої програми. Час виявлення вразливості, відомій ДНВ, t_2 = t-rand·at_2, де t – поточний час (Час виявлення вразливості – випадкова величина, що приймає з однаковою ймовірністю значення з інтервала від різниці поточного часу і часу життя вразливості до поточного часу). Варто відмітити, що принципових обмежень на вид законів розподілення в даній моделі не існує.

На відміну від моделей конфлікту, розглянутих в [17], в представленій моделі жодна зі сторін не може досягти абсолютної перемоги, тобто в разі переходу ІС 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 ІС за період конфлікту не перейде в ненадійний стан), може бути також розрахована ймовірність знаходження сторін конфлікту в певному стані (наприклад, ймовірність знаходження ІС в надійному стані).

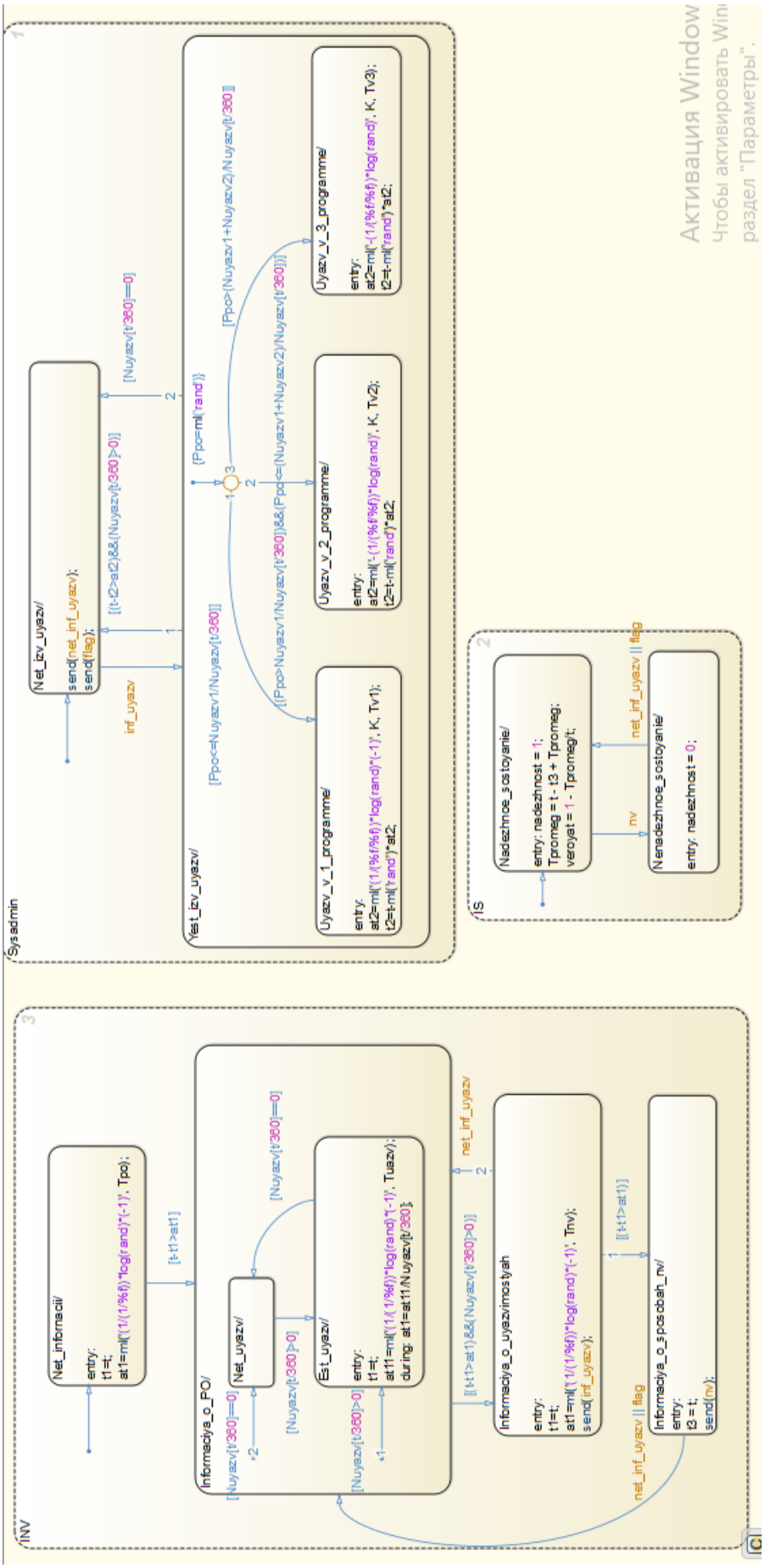


Рисунок 4.2 – SF-модель конфлікту ІС без ЗЗІ і одного ДНВ

4.2 Порівняння результатів імітаційної і математичної моделей

Щоб порівняти імітаційну і математичну моделі, пропонується розрахувати ймовірність надійності ІС і ймовірність знаходження ІС в надійному стані для кожного півріччя (передбачається, що ДНВ намагається здійснити НВ на ІС протягом цього періоду) протягом 11 років, починаючи з моменту випуску операційної системи Windows XP, за умови, що в ІС встановлена тільки операційна система Windows XP. Необхідні статистичні дані щодо ПЗ беруться з [4,18,19]. Коефіцієнт роботи системного адміністратора для визначеності береться k = 3. Розрахунок пропонується здійснити для ДНВ 4 різних рівнів кваліфікації:

- ДНВ 1-ї категорії ($T_{ПЗ}$ = 60 днів, $T_{уязв}$ = 30 днів,$T_{нв}$ = 30 днів);
- ДНВ 2-ї категорії ($T_{ПЗ}$ = 20 днів, $T_{уязв}$ = 30 днів,$T_{нв}$ = 10 днів);
- ДНВ 3-й категорії ($T_{ПЗ}$ = 10 днів, $T_{уязв}$ = 5 днів,$T_{нв}$ = 5 днів);
- ДНВ 4-ї категорії ($T_{ПЗ}$ = 5 днів, $T_{уязв}$ =1 день,$T_{нв}$ = 1 день).

Нижче на рисунках 4.1-4.4 наведені графіки ймовірності надійності і ймовірності знаходження в надійному стані ІС з операційною системою Windows 10 при спробі НВ на неї ДНВ в 1-й, 2-й, 3-й і 4-ї категорії.

Максимальне середнє абсолютне відхилення ймовірності надійності ІС, розрахованої за допомогою математичної моделі, від ймовірності надійності ІС, розрахованої за допомогою імітаційної моделі, склало 4%, а максимальне середнє абсолютне відхилення ймовірності знаходження ІС в надійному стані, розрахованої за допомогою математичної моделі, від ймовірності знаходження ІС в надійному стані, розрахованої за допомогою імітаційної моделі – 7%. Різниця в результатах при застосуванні математичної і імітаційної моделей пояснюється тим, що математична модель не враховує зміну числа вразливостей в системі протягом конфлікту. З урахуванням того, що час конфлікту передбачається рівним півроку (180 днів), останній результат означає, що різниця між середнім часом перебування ІС в надійному стані, розрахованим за

допомогою математичної і імітаційної моделей, дорівнює приблизно 13 дням, що має велике значення за умови, якщо кожен день перебування ІС в ненадійному стані несе великі матеріальні збитки компанії, що володіє цією ІС.

В кінцевому рахунку доцільність застосування математичної моделі замість імітаційної може бути обгрунтована, виходячи з оцінки ризиків, до яких може привести одноразовий успішний негативний вплив на ІС та знаходження ІС в ненадійному стані. Додатково варто відзначити, що за допомогою обох моделей може бути знайдена ймовірність порушення надійності ІС за допомогою вразливостей в конкретному ПЗ і час, необхідний ДНВ для успішного НВ на ІС, а за допомогою імітаційної моделі також кількість можливих успішних НВ на ІС та середнє максимальне час постійного перебування ІС в ненадійному стані (без повернення в надійне стан). Дані величини також можуть охарактеризувати надійність використання ПЗ в ІС в умовах конфліктних взаємодій.

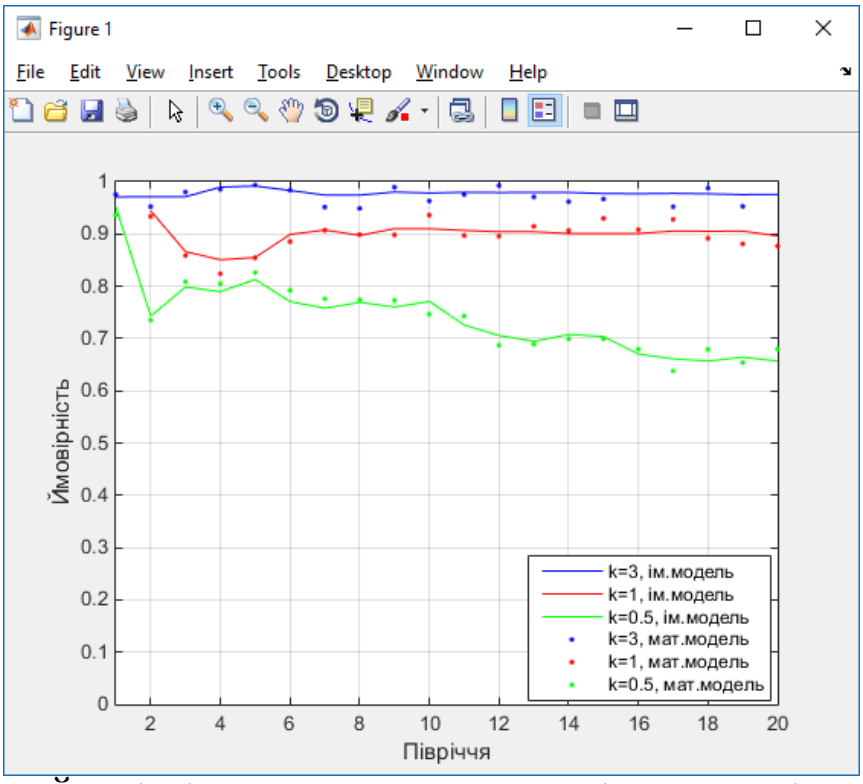


Рисунок 4.1 – Ймовірність знаходження ІС в надійному стані з операційною системою Windows XP при спробі НВ на неї ДНВ 1-й категорії і коефіцієнтах роботи системного адміністратора: k=0.5, k=1, k=3

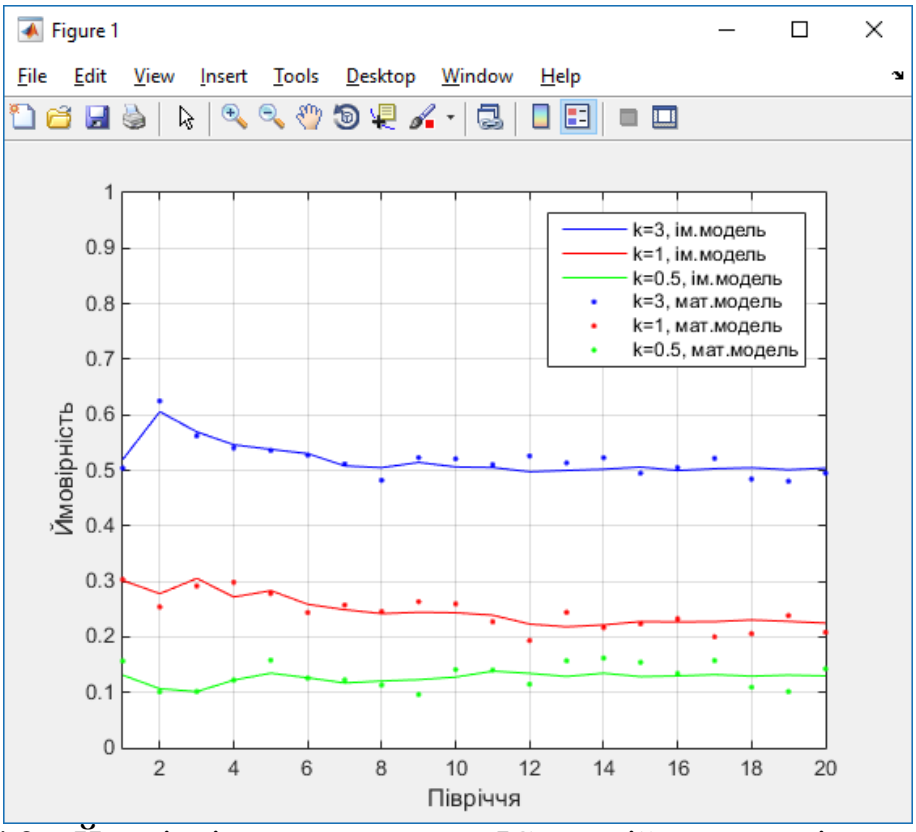


Рисунок 4.2 – Ймовірність знаходження ІС в надійному стані з операційною системою Windows XP при спробі НВ на неї ДНВ 4-й категорії і коефіцієнтах роботи системного адміністратора: k=0.5, k=1, k=3

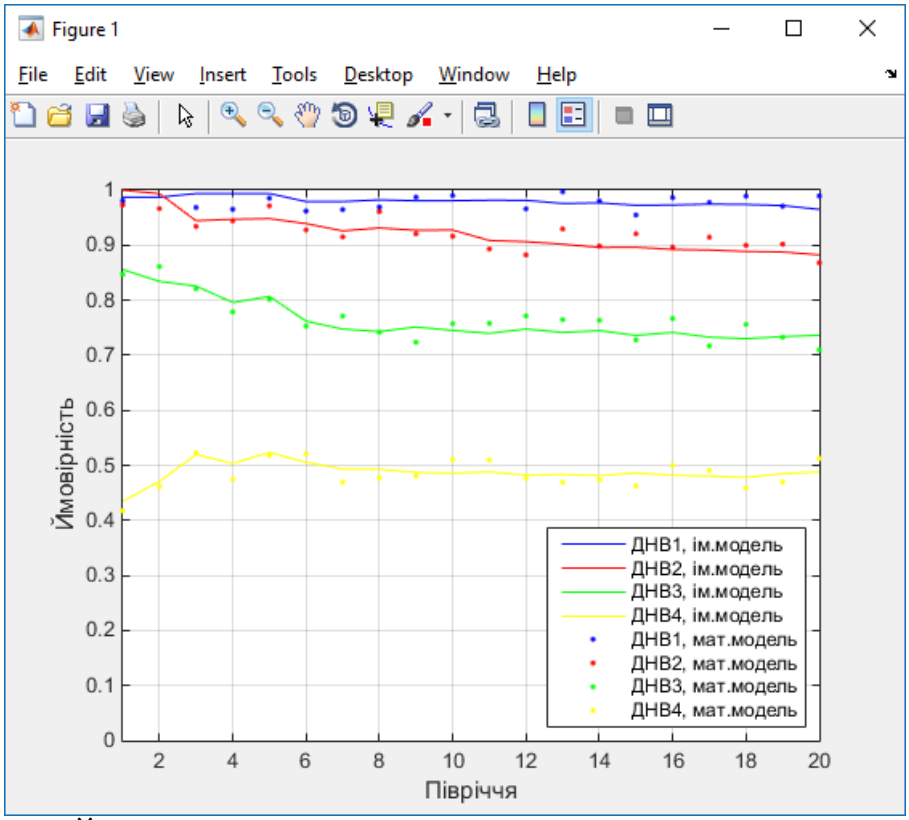


Рисунок 4.3 – Ймовірність знаходження ІС в надійному стані з операційною системою Windows XP при спробі НВ на неї ДНВ 1ї, 2ї, 3ї, 4ї категорій і коефіцієнтах роботи системного адміністратора:k=3

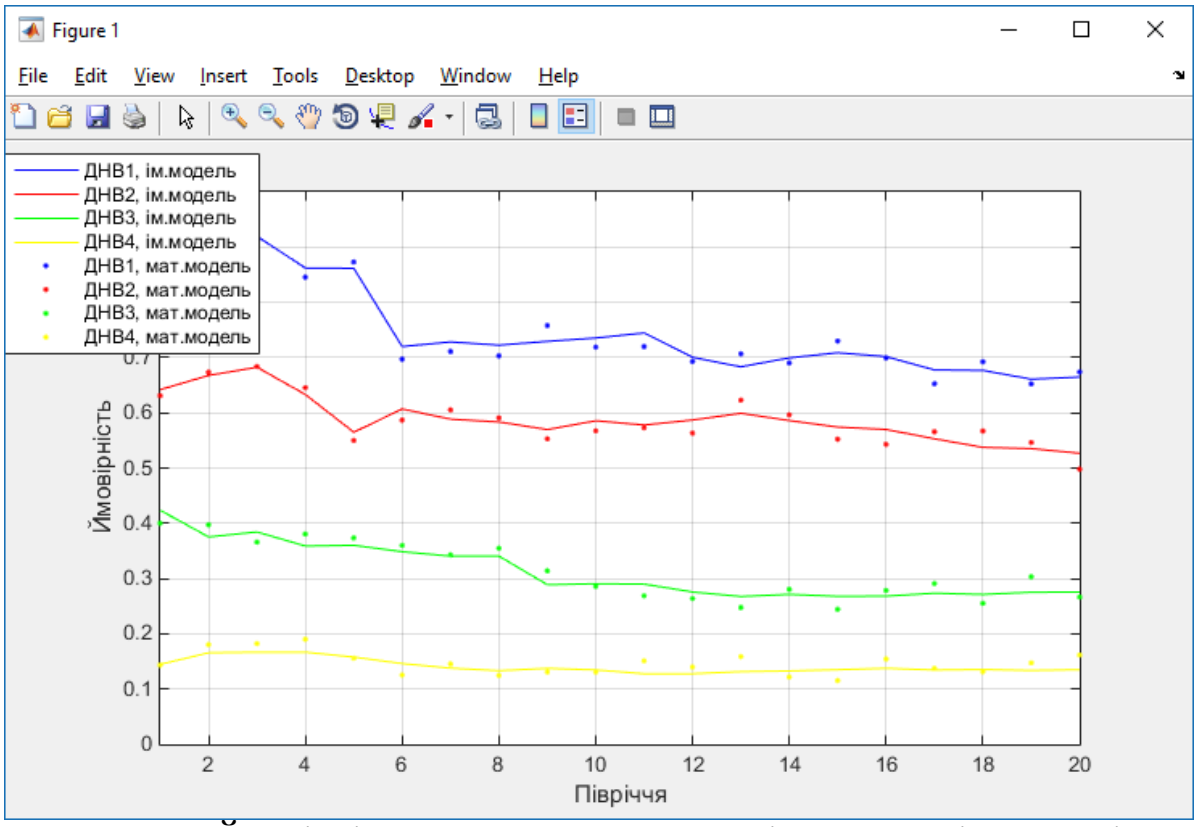


Рисунок 4.4 – Ймовірність знаходження ІС в надійному стані з операційною системою Windows XP при спробі НВ на неї ДНВ 1ї, 2ї, 3ї, 4ї категорій і коефіцієнтах роботи системного адміністратора:k=0.5

4.3 Моделювання надійності типової інформаційної системи у ТОВ «ІТЦ Ісланд-Україна»

Пропонується розглянути типову ІС працівника підприємства ТОВ «ІТЦ Ісланд-Україна», в якій встановлено наступне ПЗ (тут і далі розглядається не все ПЗ, яке може бути встановлено в ІС, а тільки основне, що є в більшості розглянутих типових елементів і містить в собі найбільшу кількість вразливостей):

– Microsoft Windows 10 (операційна система);
– Microsoft Office 2016;
– Adobe Acrobat Reader DC;

і не встановлено ЗЗІ, що перешкоджають безпосередньому НВ на ПЗ ІС. ІС може бути описана найпростішою математичною моделлю, за типом запропонованих в п.3.1, і представленої для даного конкретного випадку на рисунку 4.5.

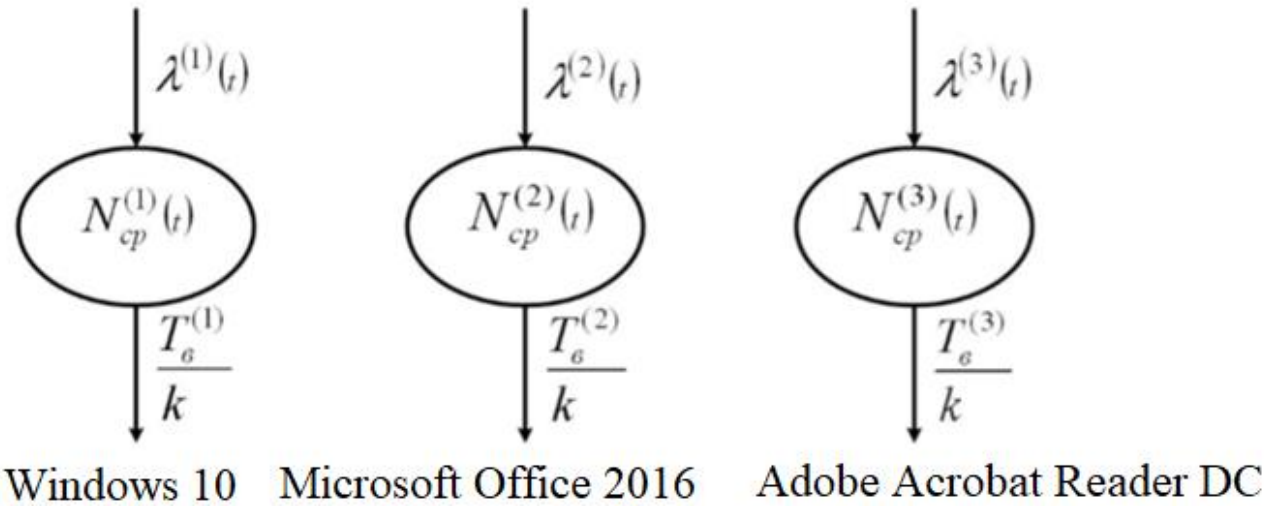


Рисунок 4.5 – модель типової ІС працівника підприємства ТОВ «ІТЦ Ісланд-Україна»

Необхідні статистичні дані для аналізу інтенсивності виявлення вразливостей в кожному конкретному ПЗ були отримані на основі даних [21, 26-28]. Для прогнозу інтенсивності виявлення вразливостей використовувався алгоритм, запропонований в п.3.1. Дані прогнозу представлені в таблиці 4.1

Таблиця 4.1 – Дані інтенсивності виявлення вразливостей

ПЗ / Місяць	Microsoft Windows 10	Microsoft Office 2016	Adobe Acrobat Reader DC
Вересень 2016	1,7	1,5	2,8
Жовтень 2016	1,0	1,4	15,1
Листопад 2016	1,3	1,3	19,6
Грудень 2016	2,4	1,2	13,3
Січень 2017	4,3	1,0	8,8
Лютий 2017	7,2	0,7	12,4

Виходячи зі статистистичних даних [21, 26-28], середній час усунення вразливостей вендором з Windows 10 становить 19,4 дні, з Microsoft Office 2016 – 54 дні, з Adobe Acrobat Reader DC – 9 днів. Оскільки точні дані ПЗ роботі системних адміністраторів типових ІС користувачів і ДНВ, які могли б негативно впливати на них, відсутні, пропонується здійснити прогноз для коефіцієнта роботи системного адміністратора від 0 до 3 с кроком 0,1 і наступних ДНВ [22-23]:

– ДНВ 1-ї категорії ($T_{ПЗ}$ = 60 днів, $T_{уязв}$ = 30 днів,$T_{нв}$ = 30 днів);
– ДНВ 2-ї категорії ($T_{ПЗ}$ = 20 днів, $T_{уязв}$ = 30 днів,$T_{нв}$ = 10 днів);
– ДНВ 3-й категорії ($T_{ПЗ}$ = 10 днів, $T_{уязв}$ = 5 днів,$T_{нв}$ = 5 днів);
– ДНВ 4-ї категорії ($T_{ПЗ}$ = 5 днів, $T_{уязв}$ =1 день,$T_{нв}$ = 1 день).

Передбачається, що на ІС буде наносити НВ тільки один ДНВ, крім того, як вже було сказано, ЗЗІ, що перешкоджають безпосередньому НВ на ПЗ в ІС, відсутні, отже, для моделювання конфлікту ІС і ДНВ можна використовувати імітаційну модель.

Далі наведено прогноз ймовірності надійності і ймовірності знаходження в надійному стані типової ІС користувача системою, а саме працівника підприємства ТОВ «ІТЦ Ісланд-Україна».

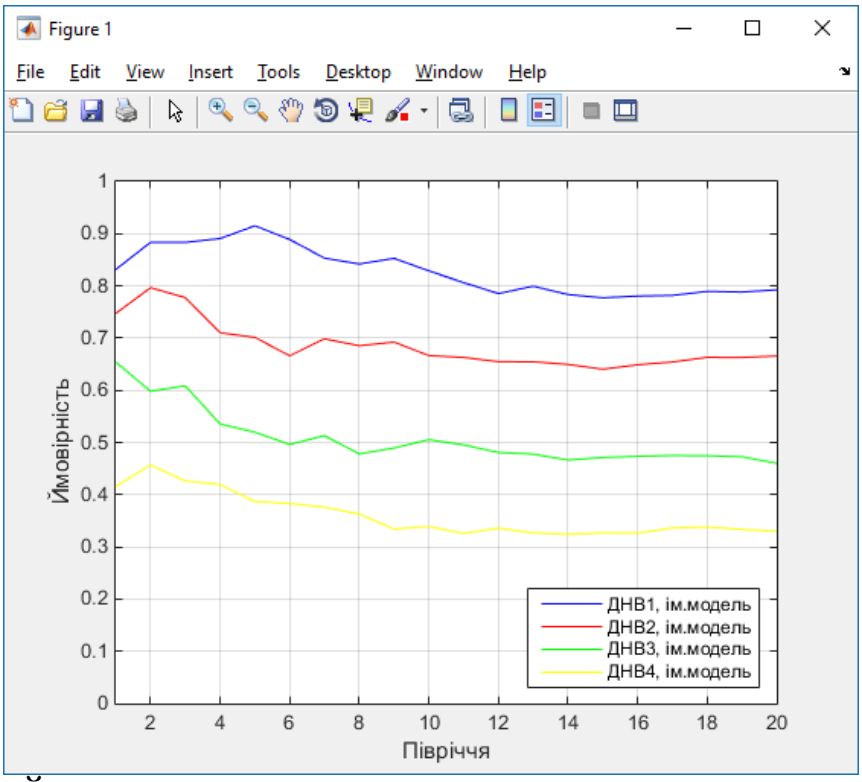


Рисунок 4.6– Ймовірність знаходження ІС в надійному стані при спробі НВ на неї ДНВ 1ї, 2ї, 3ї, 4ї категорій і коефіцієнтах роботи системного адміністратора:k=3

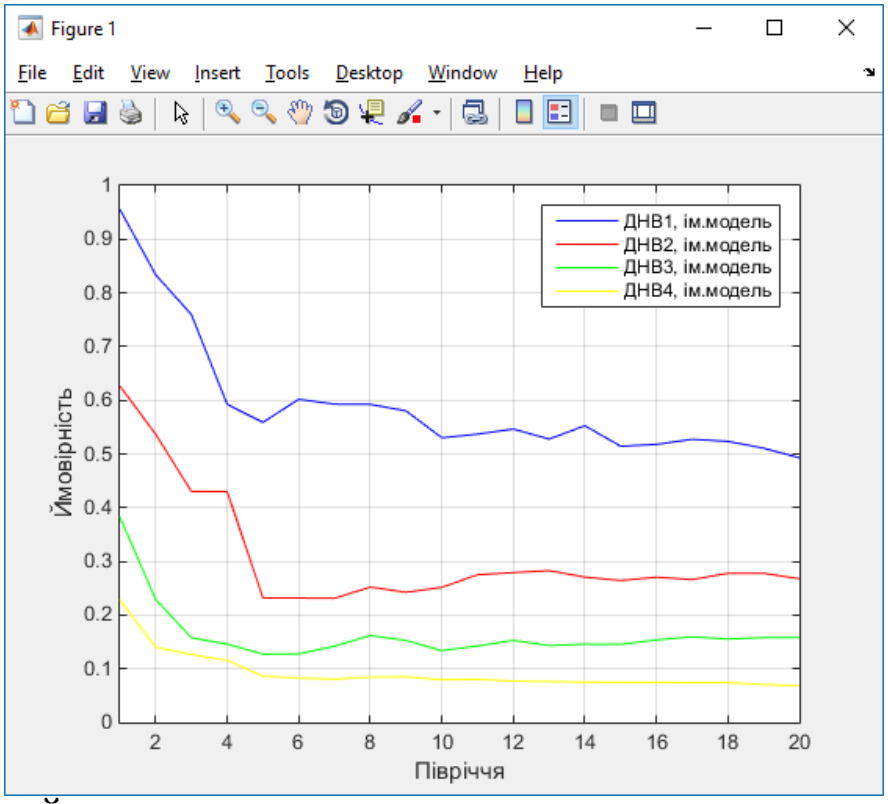


Рисунок 4.8 – Ймовірність знаходження ІС в надійному стані при спробі НВ на неї ДНВ 1ї, 2ї, 3ї, 4ї категорій і коефіцієнтах роботи системного адміністратора:k=0.5

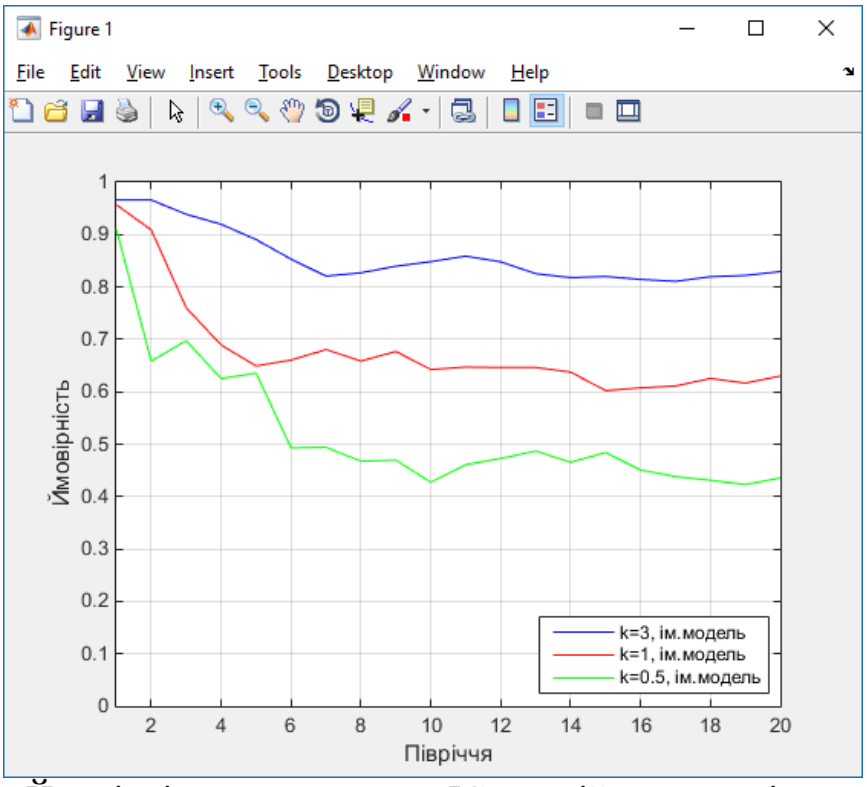


Рисунок 4.9 – Ймовірність знаходження ІС в надійному стані при спробі НВ на неї ДНВ 1ї категорій і коефіцієнтах роботи системного адміністратора:k=3, k=1. k=0.5

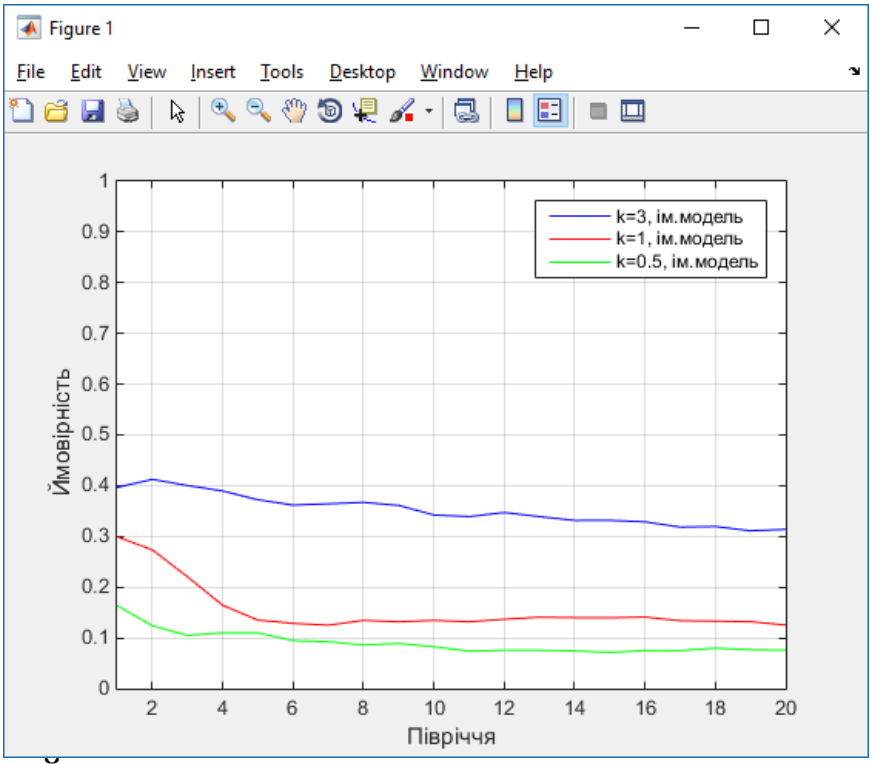


Рисунок 4.10 – Ймовірність знаходження ІС в надійному стані при спробі НВ на неї ДНВ 4ї категорій і коефіцієнтах роботи системного адміністратора:k=3, k=1, k=0.5

Аналізуючи отримані графіки, можна зробити наступні висновки:

– якщо на ІС буде здійснено НВ ДНВ 1ї категорії, то в 90% випадках система може справно функціонувати, тобто залишитись в надійному стані;

– ймовірність того, що система залишиться в надійному стані вище, якщо за нею доглядає системний адміністратор з вищою кваліфікацією. Своїми діями він може закрити вразливе місце, встановити ЗЗІ або ж самостійно написати патч;

– якщо системою займається служба безпеки (вкрай рідкісний випадок), в яку входить велика кількість висококваліфікованих співробітників, і застосовуються додаткові організаційні та технічні заходи щодо усунення вразливостей з ПО (коефіцієнт роботи системного адміністратора дорівнює 3), то навіть при спробах НВ з боку ДНВ 1-ї категорії робота ІС буде порушена в середньому протягом 1/10 періоду;

– якщо в системі налаштоване автоматичне оновлення ПЗ (коефіцієнт роботи системного адміністратора дорівнює 1), то навіть при спробах НВ з боку ДНВ 1-ї категорії робота ІС буде порушена в середньому протягом 1/5 періоду прогнозу;

– якщо системний адміністратор зовсім не оновлює ПЗ, встановлене в ній (коефіцієнт роботи системного адміністратора дорівнює 0.5), то навіть при спробах НВ з боку ДНВ 1-ї категорії в робота ІС буде порушена в середньому робота ІС буде порушена більшу частину періоду.

Таким чином, ІС є ненадійною, і потрібні додаткові заходи щодо забезпечення її захисту. Для підвищення надійності даної ІС рекомендується обмежити програмне забезпечення ІС тільки довіреним обличчям і тим, які реалізують необхідний функціонал (у тому числі обмежити мережеві протоколи та мережеві взаємодії тільки необхідними довіреними вузлами), що забезпечується відповідними налаштуваннями операційної системи. А також необхідно встановити ЗЗІ, інтенсивність виявлення вразливостей, в якому мала і яке перешкоджає безпосередньому НВ на програмне забезпечення ІС. У іншому випадку ніяких гарантій працездатності ІС протягом періоду прогнозу дати не можна.

ВИСНОВКИ

Запропоновано математичні моделі динаміки станів програм і інформаційної системи з урахуванням можливих вразливостей, що враховують залежності інтенсивностей виявлення вразливостей від часу, часових характеристик закриття вразливостей від роботи виробника програмного забезпечення і адміністратора інформаційної системи.

Розроблено об'єктно-орієнтовані і математичні моделі інформаційної системи в динаміці конфліктної взаємодії, імітаційні моделі використання динаміки конфліктної взаємодії.

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.

Результати дозволяють:

– користувачам інформаційних систем – виявити слабкі місця в політиці забезпечення надійності (оцінити роботу системного адміністратора, виявити програмне забезпечення, використання якого небажано, і т.п.), оцінити матеріальні та інші ризики, яким може піддатися інформаційна система , а також виробити рекомендації щодо їх зменшення;

– розробникам програмного забезпечення – раціонально розподіляти фінансові та інші ресурси при підтримці існуючого програмного забезпечення та розробці нового;

– організаціям, що здійснюють атестацію інформаційних систем і сертифікацію програмного забезпечення – точніше оцінити реальні процеси функціонування інформаційних систем в умовах конфліктних взаємодій, виробити на основі розроблених моделей і алгоритмів нову методологію, більш повно враховує дані процеси.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Okamura, H. 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.

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. Frei, S. Security econometrics – the dynamics of security: dissertation for the degree of Doctor of Science / Stefan Frei. ETH Zurich, 2009. 184 p.

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

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

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

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

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

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. Кельберт, М. Я. Імовірність і статистика в прикладах і задачах. Т. II: Марківські ланцюги як відправна точка теорії випадкових процесів та їх застосування / М.Я. Кельберт, Ю.М. Сухов. - М .: МЦНМО, 2009. 295 с.

15. 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.

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

17. Алгазінов, Є.К. Аналіз і комп'ютерне моделювання інформаційних процесів і систем / Е. К. Алгазіна, А. А. Сирота. За заг. ред. А. А. Сироти. М Діалог-МІФІ, 2009. 416 с.

18. Microsoft Corp . URL: http://microsoft.com.

19. The Open Source Vulnerability Database . URL: http://osvdb.org.

20. Організація роботи GanttProject. URL: http://pro-spo.ru/textl/141-ganttproject

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

22. 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.

23. Форум CRACK FORUM // CRACK FORUM. URL: http://www.crack-forum.com.

24. Joh, H. Seasonality in Vulnerability Discovery in Major Operating Systems and Web Applications / H. Joh, Y.K. Malaiya // Fast Abstract, Proc. Int. Symp. Software Reliability Eng., Nov. 2008. pp. 297-298.

25. Joh, H. Seasonal Variation in the Vulnerability Discovery Process / H. Joh, Y.K. Malaiya // Proc. 2nd IEEE Int. Conf. Software Testing, Verification, and Validation, April 2009. pp. 191-200.

26. Microsoft Security Intelligence Report v14 // Mictosoft. URL: http://www.microsoft.com/security/sir/.

27. Microsoft Security Intelligence Report v15 // Mictosoft. URL: http://www.microsoft.com/security/sir/.

28. Internet Security Threat Report 2016 Trends // Symantec. URL: http://owasp.com/images/7/70/Symantec_ISTR_17.pdf.

29. Тихонов, В.І. Марківські процеси / В.І. Тихонов, М.А. Миронов. М.: «Сов. радио», 1977. 488 с.

30. Stateflow // Symantec. URL: https://matlab.ru/products/stateflow

31. Stateflow 5. Руководство пользователя // Symantec. URL: http://matlab.exponenta.ru/stateflow/book1/2.php

32. How to Build a Simple StateflowModel // Symantec. URL: https://www.ethz.ch/content/dam/ethz/special-interest/mavt/dynamic-systems-n-control/idsc-dam/Lectures/Embedded-Control-Systems/OtherNotes/Stateflow_Modelling.pdf

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

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

35. Всеукраїнський конкурс студентських наукових робіт зі спеціальності «Комп’ютерні науки» (Харків, 24-26 квітня 2019 року) Веб-сайт. URL: http://nure.ua/wp-content/uploads/Main_Docs_NURE/skr_nadiia.pdf

ДОДАТОК А ТЕХНІЧНЕ ЗАВДАННЯ

ТЕХНІЧНЕ ЗАВДАННЯ

на створення математичної моделі, об’єктно-орієнтованих моделей та імітаційної моделі за темою«Комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій»

1 Найменування: комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій

2 Терміни виконання: 10 червня 2019 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 математичну, об’єктно-орієнтовані та імітаційну моделі конфлікту ПЗ в ІС в інформаційній системі з джерелом негативного впливу.

5 Основні завдання: модель дозволяє імітувати та прогнозувати конфліктні взаємодії інформаційних систем з джерелами негативного впливу.

6 Вхідні дані: коефіцієнт діяльності системного адміністратора, середній час, необхідний ДНВ для знаходження інформації про спосіб використання вразливості в ПЗ ІС для негативного впливу на ІС, середній час, необхідний ДНВ для знаходження всіх вразливостей в ІС, середній час, необхідний ДНВ для знаходження інформації про ПЗ ІС.

7 Вихідні дані: графік надійності інформаційної системи та графік прогнозування її надійності у майбутньому.

8 Програмне забезпечення: побудова напівмарківської моделі – Microsoft Visio 2016, розробка об’єктно-орієнтованих моделей – Visual Studio 2015, розробка імітаційної моделі – Matlab P2014b 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 Б ПЛАНУВАННЯ РОБІТ

Б.1 Ідентифікація ідеї проекту

Ускладнення завдань, що виконуються сучасними інформаційними системами, розвиток використовуваних у них інформаційних технологій, а також виникнення умов функціонування вимагає нових підходів до аналізу та прогнозування надійності ІС. Підходи, які використовуються, не враховують як динаміку вразливостей в інформаційних системах, так і динаміку навмисного негативного впливу на інформаційні системи або ж моделюють їх без урахування ряду важливих факторів, які проявляються саме в умовах конфліктної взаємодії.

Метою є розробка моделі і алгоритму аналізу та прогнозування надійності використання програмного забезпечення в інформаційних системах в умовах конфліктних взаємодій.

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

Б.2 Деталізація мети методом SMART

Щоб провести деталізацію мети використовують метод SMART, який в менеджменті та управлінні проетами дозволяє визначити цілі та поставити завдання. Сутність деталізації мети проекту за допомогою SMART-методу випливає з розшифровки термінів, які формують його назву: конкретна мета (Specific), вимірювана (Measurable), досяжна (Achievable), реалістична (Relevant), обмежена у часі (Time-framed). Результати деталізації наведені у таблиці Б.1

Таблиця Б.1 – Деталізація мети методом SMART

Specific (конкретна)	Створити математичну, об’єктно-орієнтовані та імітаційну модель конфлікту «інформаційна система – джерело негативного впливу»
Measurable (вимірювана)	Результатом будуть моделі і алгоритми і можливість прогнозування найбільш важливих факторів, що впливають на надійність використання ПЗ в ІС в умовах конфліктних взаємодій
Achievable (досяжна)	Для досягнення мети необхідно розробити моделі конфлікту «інформаційна система – джерело негативного впливу», а також на її основі створити імітаційну модель
Relevant (реалістична)	У наявності є всі необхідні технічні та програмні засоби. Розробники достатньо кваліфіковані для виконання поставлених задач.
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 ПЗ в ІС в умовах конфліктних взаємодій до 4 червня 2019 року.

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

Запропоновані математичні моделі динаміки станів програм і інформаційної системи з урахуванням можливих вразливостей, що враховують

залежності інтенсивностей виявлення вразливостей від часу, часових характеристик закриття вразливостей від роботи виробника програмного забезпечення і адміністратора інформаційної системи. Також розроблені об'єктно-орієнтовані моделі інформаційної системи в динаміці конфліктної взаємодії, імітаційні моделі використання динаміки конфліктної взаємодії. Модель дозволяє обирати стратегії вирішення конфліктних взаємодій в інформаційних системах.

На відміну від існуючих аналітичних моделей виявлення вразливостей запропоновані моделі забезпечують 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.

Результати дозволяють:

– користувачам інформаційних систем – виявити слабкі місця в політиці забезпечення надійності (оцінити роботу системного адміністратора, виявити програмне забезпечення, використання якого небажано, і т.п.), оцінити матеріальні та інші ризики, яким може піддатися інформаційна система , а також виробити рекомендації щодо їх зменшення;

– розробникам програмного забезпечення – раціонально розподіляти фінансові та інші ресурси при підтримці існуючого програмного забезпечення та розробці нового;

– організаціям, що здійснюють атестацію інформаційних систем і сертифікацію програмного забезпечення – точніше оцінити реальні процеси функціонування інформаційних систем в умовах конфліктних взаємодій, виробити на основі розроблених моделей і алгоритмів нову методологію, більш повно враховує дані процеси.

Б.4 Попередній опис змісту проекту

– Аналіз умов функціонування інформаційних систем;

– аналіз процесу виявлення та усунення вразливостей;

– аналіз методів виявлення та усунення вразливостей;

– розробка математичних моделей інформаційних систем в умовах конфліктних взаємодій;

– математична модель функціонування інформаційних систем в умовах внутрішніх вразливостей і конфліктних взаємодій;

– математична модель конфлікту інформаційних систем без засобів захисту інформації і джерела негативного впливу;

– об’єктно-орієнтована модель конфліктної взаємодії;

– комп’ютерна технологія моделювання процесів конфліктних взаємодій;

– розробка імітаційної моделі конфлікту інформаційної системи і джерела негативного впливу;

– результати імітаційної моделі.

Б.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 ПЗ в ІС;

– визначення основних вимог до розроблюваних алгоритмів і моделей аналізу надійності використання ПЗ в ІС в умовах конфліктних взаємодій;

– аналіз сучасних підходів до оцінки надійності використання ПЗ в ІС на предмет врахування даних факторів і вимог;

– розробка моделей функціонування інформаційних систем при наявності внутрішніх вразливостей;

– розробка алгоритмів і моделей оцінки надійності використання ПЗ в ІС 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 ПЗ в ІС та ДНВ.

Б.6 Планування змісту 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, ПЗ якій керівник проекту завжди може визначити, чи всі проміжні точні результати, що ведуть до досягнення мети проекту, враховані[30].

Створена WBS-діаграма представлена на рисунку Б.1.

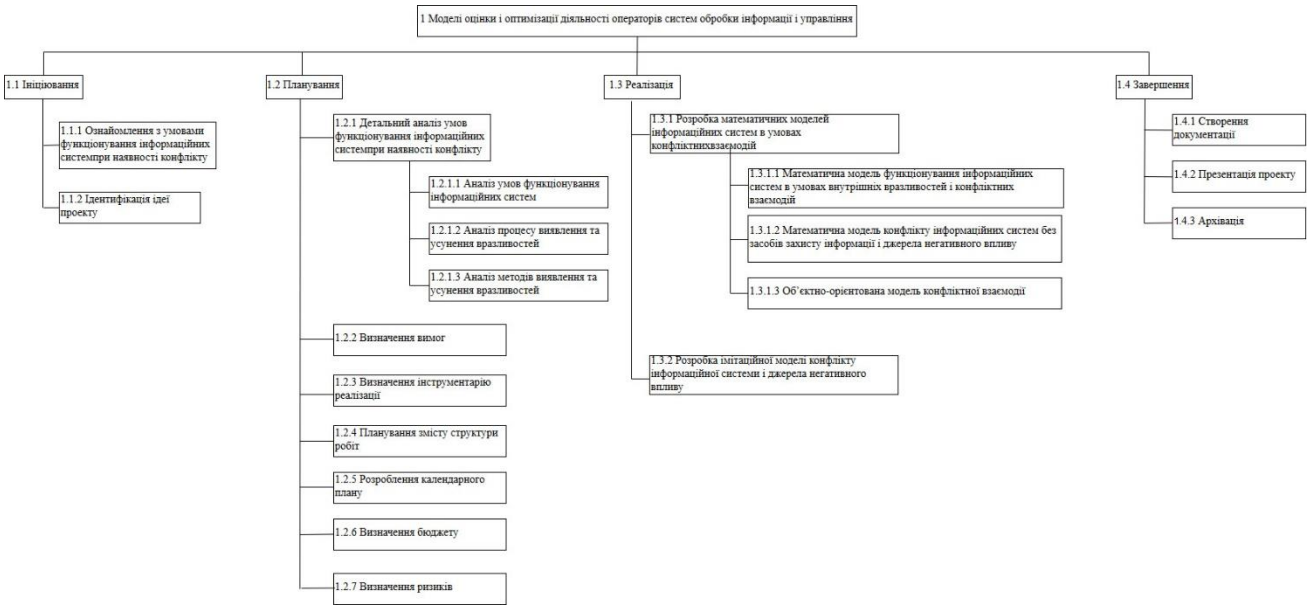


Рисунок Б.1 – WBS структура проекту

Б.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[31].

У проекті створення і автоматизованої система прокату та обліку авто були задіяні наступні виконавці:

– студент Щербань Тетяна Володимирівна – розробник;

– професор Лавров Євгеній Анатолійович – керівник проекту;

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

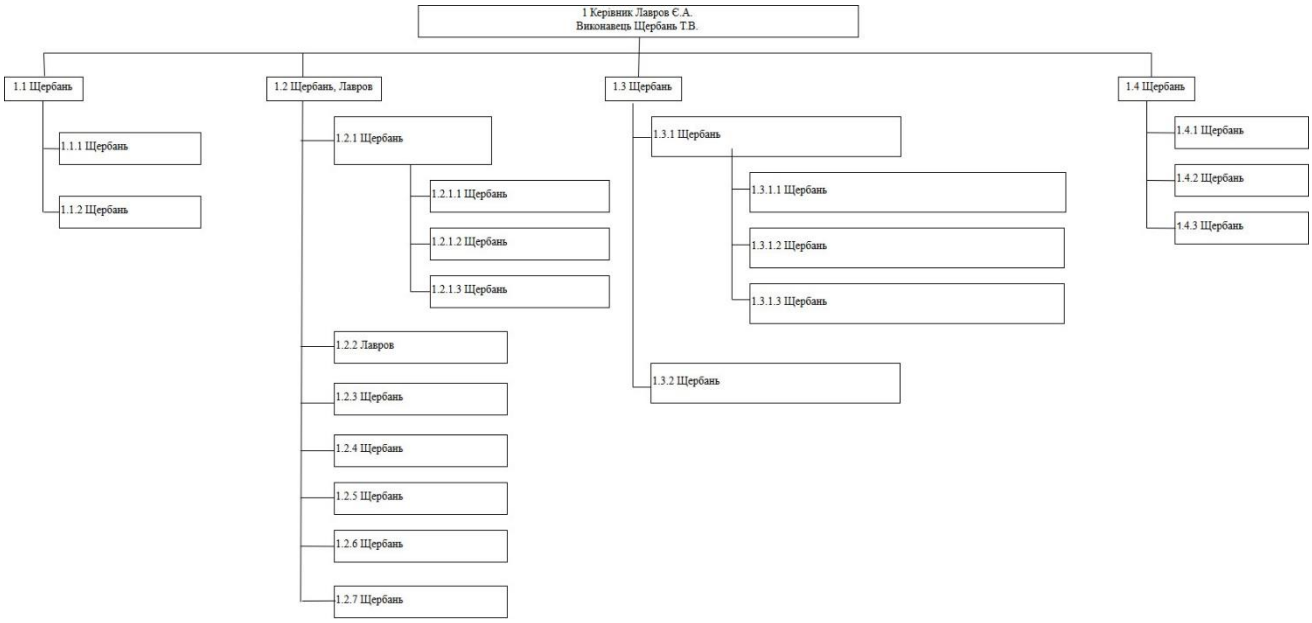


Рисунок Б.2 – OBS структура

Б.8 Побудова матриці відповідальності

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

На рисунку Б.3 показано матрицю відповідальності проекту.

	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	CP1.4.1	CP1.4.2	CP1.4.3
			CP1.2.1.1	CP1.2.1.2	CP1.2.1.3							CP1.3.1.1	CP1.3.1.2	CP1.3.1.3				
Щербань Т.В.	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
Лавров Є.А.						+												

Рисунок Б.3 – Матриця відповідальності

Б.9 Побудова календарного графіку

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 Б.4-Б.5.

Название	Дата начала	Дата с
1 Моделі оцінки і оптимізації діяльності операторів систем обробки інформації і управління	15.04.19	04.06.19
1.1 Ініціювання	15.04.19	16.04.19
1.1.1 Ознайомлення з умовами функціонування інформаційних систем при наявності конфлікту	15.04.19	15.04.19
1.1.2 Ідентифікація ідеї проекту	16.04.19	16.04.19
1.2 Планування	17.04.19	30.04.19
1.2.1 Детальний аналіз умов функціонування інформаційних системпри наявності конфлікту	17.04.19	24.04.19
1.2.1.1 Аналіз умов функціонування інформаційних систем	17.04.19	18.04.19
1.2.1.2 Аналіз процесу виявлення та усунення вразливостей	19.04.19	22.04.19
1.2.1.3 Аналіз методів виявлення та усунення вразливостей	23.04.19	24.04.19
1.2.2 Визначення вимог	25.04.19	26.04.19
1.2.3 Визначення інструментарію реалізації	25.04.19	26.04.19
1.2.4 Планування змісту структури робіт	29.04.19	29.04.19
1.2.5 Розроблення календарного плану	29.04.19	29.04.19
1.2.6 Визначення бюджету	30.04.19	30.04.19
1.2.7 Визначення ризиків	30.04.19	30.04.19
1.3 Реалізація	01.05.19	04.06.19
1.3.1 Розробка математичних моделей інформаційних систем в умовах конфліктнихвзаємодій	01.05.19	21.05.19
1.3.1.1 Математична модель функціонування інформаційних систем в умовах внутрішніх вразливостей і конфліктних взаємодій	01.05.19	07.05.19
1.3.1.2 Математична модель конфлікту інформаційних систем без засобів захисту інформації і джерела негативного впливу	08.05.19	14.05.19
1.3.1.3 Об'єктно-орієнтована модель конфліктної взаємодії	15.05.19	21.05.19
1.3.2 Розробка імітаційної моделі конфлікту інформаційної системи і джерела негативного впливу	22.05.19	04.06.19
1.4 Завершення	23.04.19	04.06.19
1.4.1 Створення документації	23.04.19	03.06.19
1.4.2 Презентація проекту	27.05.19	03.06.19
1.4.3 Архівація	04.06.19	04.06.19

Рисунок Б.4 – Весь список робіт для побудови діаграми

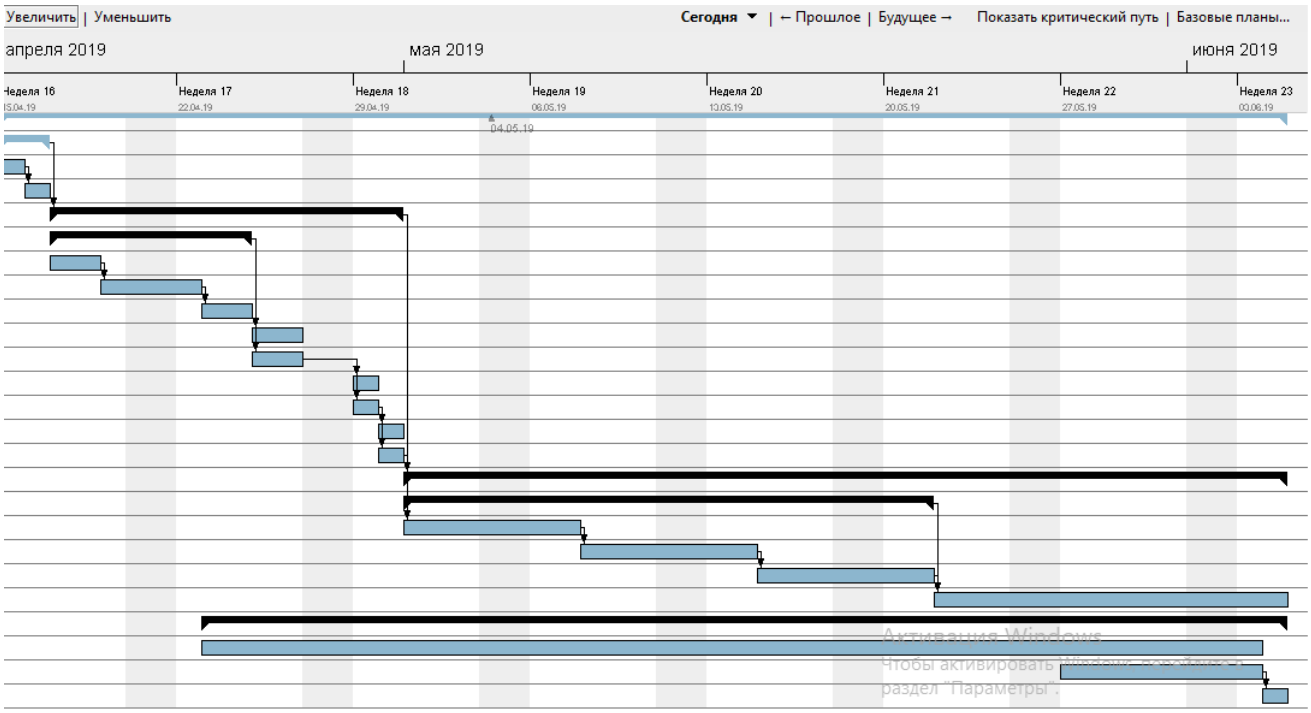


Рисунок Б.5 – Діаграма Ганта

Б.10 Управління ризиками 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 захистити проект від негативних факторів і небезпек, необхідно розробити продуману стратегію управління ризиками.

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 В.6 та у таблицях Б.2-Б.3.

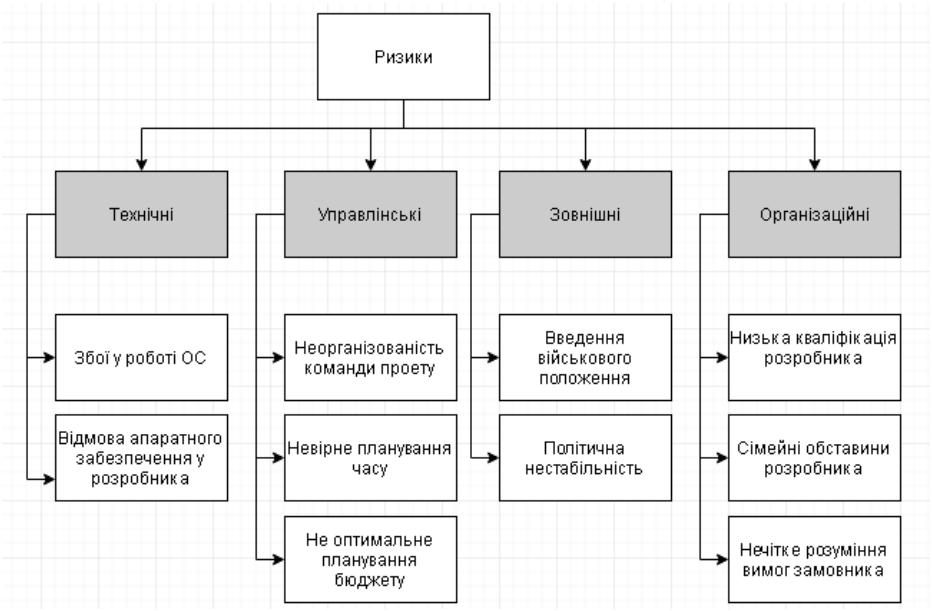


Рисунок Б.6– Діаграма ризиків проекту

Таблиця Б.2– Визначення характеристик ризиків

Назва	**Імовірність**	**Втрати**	**Вплив**	**Характер**
Збої у роботі ОС	1	2	4	Ігноровані
Відмова апаратного забезпечення у розробника	1	4	8	Незначні
Неорганізованість команди проекту	2	4	8	Незначні
Невірне планування часу	3	4	10	Значні
Не оптимальне планування бюджету	3	5	10	Значні
Політична нестабільність	3	4	4	Ігноровані
Низька кваліфікація розробника	1	4	6	Ігноровані
Сімейні обставини розробника	2	5	8	Помірні
Нечітке розуміння вимог замовника	3	4	10	Значні

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

Ризики проекту	**План запобігання ризику**	**Мінімізація наслідків**
Невірне планування часу	Оптимізувати розподіл часу. За необхідності найняти спеціаліста.	Намагатися раціонально використати час, що залишився
Не оптимальне планування бюджету	Своєчасна перевірка кошторисів	Компенсувати втрати за рахунок інших етапів проекту.
Сімейні обставини розробника	При плануванні термінів робіт виділити декілька днів для резерву.	Знайти спеціаліста, який би замінив розробника на деякий час.
Нечітке розуміння вимог замовника	Виділити більше часу на обговорення задачі проекту та його етапів, скласти глосарій термінів. Знайти дистанційний спосіб комунікації	Вчасно знайти невідповідність та обговоривши з замовником зробити необхідні правки

Б.11 Формування бюджету проекту

Бюджетування проекту – це визначення вартісних значень виконуваних в рамках проекту робіт і проекту в цілому, процес формування бюджету проекту, що містить встановлений (затверджений) розподіл витрат за видами робіт, статтями витрат, за часом виконання робіт, за центрами витрат або ПЗ іншій структурі. Структура бюджету визначається планом рахунків вартісного обліку конкретного проекту. Далі бюджет ІТ-проекту розраховується як сумарна вартість годин затрачених на розробку проекту, також додаються ризики (до 20%) та вартість проекту [34].

Опис робіт та планування бюджету представлені в таблиці Б.4 Вартістю виконання робіт були прийняті середні ціни на ринку ІТ-послуг у м.Суми.

Таблиця Б.4 – Опис робіт та планування бюджету

Задача	**Кількість днів**	**Оплата за день**	**Ціна**
Математична модель функціонування інформаційних систем в умовах внутрішніх вразливостей і конфліктних взаємодій	5	150	750
Математична модель конфлікту інформаційних систем без засобів захисту інформації і джерела негативного впливу	5	150	750
Об’єктно-орієнтована модель конфліктної взаємодії	5	200	1000
Розробка імітаційної моделі конфлікту інформаційної системи і джерела негативного впливу	10	300	3000
Результати імітаційної моделі	5	100	500
Створення документації + презентація	35	200	7000
		Сума:	**13000**

ДОДАТОК В АКТИ ВПРОВАДЖЕННЯ

АКТ
впровадження результатів наукової роботи
«КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ КОНФЛІКТНИХ ВЗАЄМОДІЙ»
у процес підтримки програмного комплексу «1С:Підприємство»
ТОВ «ІТЦ Ісланд-Україна» у 2018 р.

Комісія у складі: директора Харченко В'ячеслава Вікторовича та члену комісії Федорченко Костянтина Олександровича склали цей акт у тому, що результати студентської наукової роботи автора Щербань Т.В. на тему «Комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій» для організації підтримки програмного комплексу «1С:Підприємство».

Авторами роботи вирішується актуальна науково-практична задача розробки моделі підтримки прийняття рішень, яка базується на алгоритмі оптимізації, що враховує ймовірнісний характер часового ресурсу та максимізує безпомилковість виконання операції. Практична значимість роботи представлена розробленим програмним забезпеченням.

Результати студентської наукової роботи передбачається використовувати при обробці запитів клієнтів для знаходження ліпшого шляху вирішення проблеми з використанням існуючої бази знань підприємства та гарантуючи вчасність виконання. Розроблене програмне забезпечення може бути запропоновано для впровадження в інших інформаційно-технологічних центрах.

Директор В.В. Харченко

Інженер-програміст К.О. Федорченко

Затверджую
Перший проректор
Сумського державного
університету
_____ Карпуша В.Д.
«___» _____ 2019 р.

Акт
Впровадження в навчальний процес
СУМСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ
результатів наукової роботи
студентки групи ІТ-51 Сумського державного університету
Щербань Тетяна Володимірівна
на тему
«Комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій»

Складений 5 січня 2019 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. Старший викладач кафедри *комп'ютерних наук, кандидат технічних наук,* **Кузнєцов Е.Г.**

В період з 3 січня 2019 р. по 5 січня 2019 р. комісія провела роботу з визначення впровадження результатів Щербань Т.А. в навчальний процес кафедри комп'ютерних наук.

Результати роботи комісії

1. На кафедру комп'ютерних наук передано комплекс програм «Комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій».
2. Матеріали використні в дисциплінах:
   - **«Системи підтримки прийняття рішень»** для слухачів магістратури, що навчаються за спеціальністю «Інформатика», при розробці теми **«Прийняття рішень в умовах ризику»** (лабораторна робота – 2 год.).
   - **«Організація людино-машинної взаємодії»** для слухачів магістратури, що навчаються за спеціальністю «Інформаційні технології проектування», при розробці теми **«Ергономіка автоматизованих виробництв»** (лабораторна робота – 2 год.).

Голова комісії _____
Члени комісії _____
_____
_____
_____

ДОДАТОК Г 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. Дякулій 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. Имеется ввиду, 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-темповая 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 полным и достоверным набором 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 является 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-руководителям. Известные программы не позволяют оператору-руководителю в условиях информационной напряженности и дефицита времени оценить последствия распределения работ и выбрать оптимальный вариант.

Основными проблемами являются:

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

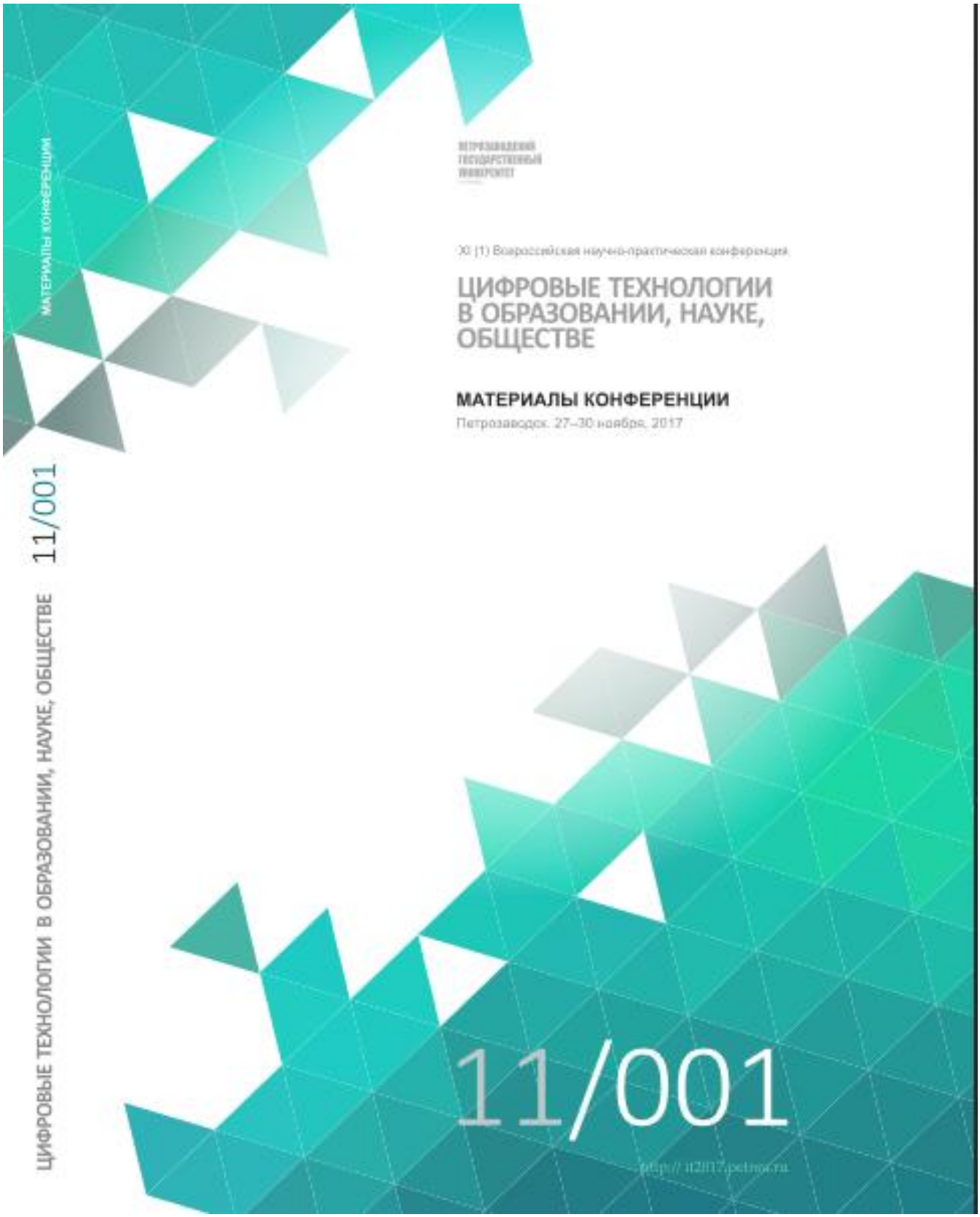
В связи с этим нами разрабатываются элементы СППР, позволяющие:

- 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 База 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 эргатехнических 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.Б., Плеханов 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-машинным взаимодействием// 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
XI (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
- темповые 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 CUM.

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, испытание: 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. Кривдуб 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

UNITECH 2017 GABROVO

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,

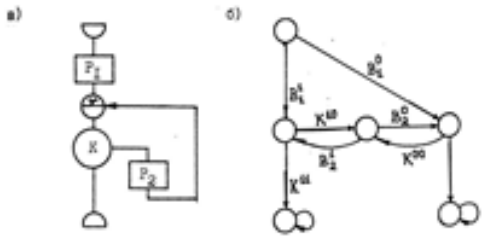
K– performance control operation

$B_i^1(B_i^0)$ - 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_i - 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)

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