НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО
ІНФОРМАЦІЙНОГО ПРОСТОРУ

**СКЛАДАННИЙ ПАВЛО МИКОЛАЙОВИЧ**

УДК 004.056.5:681.51

# МОДЕЛІ І МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІМІТОСТІЙКОСТІ ТА КОНФІДЕНЦІЙНОСТІ В СИСТЕМАХ ОБРОБКИ ІНФОРМАЦІЇ

Спеціальність 05.13.06 – Інформаційні технології

**АВТОРЕФЕРАТ**

дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана на кафедрі інформаційної та кібернетичної безпеки факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
**Гулак Геннадій Миколайович,**
завідувач лабораторії досліджень з питань кібербезпеки
Інститут проблем математичних машин і систем Національної академії наук України

Офіційні опоненти: доктор технічних наук, професор
**Рудницький Володимир Миколайович**
завідувач кафедри
інформаційної безпеки та комп'ютерної інженерії
факультету інформаційних технологій і систем
Черкаського державного технологічного університету

доктор технічних наук, доцент
**Зибін Сергій Вікторович,**
завідувач кафедри інженерії програмного забезпечення
факультету кібербезпеки,
комп'ютерної та програмної інженерії
Національного авіаційного університету

Захист дисертації відбудеться «25» березня 2021 року о 13 годині на засіданні спеціалізованої вченої ради Д 26.255.01 в Інституті телекомунікацій і глобального інформаційного простору НАН України за адресою: 03186, м. Київ, Чоколівський бульвар, буд. 13, к.601.

З дисертацією можна ознайомитись у бібліотеці Інституту телекомунікацій і глобального інформаційного простору НАН України за адресою: 03186, м.Київ, Чоколівський бульвар, буд. 13.

Автореферат розісланий «___» лютого 2021 року.

Учений секретар СВР Д 26.255.01
к.т.н., ст. дослідник О.Г. Лебідь

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми.** У сучасному світі спостерігається постійне зростання сфер застосування різноманітних автоматизованих систем обробки інформації (СОІ). СОІ забезпечують постійне функціонування об'єктів сектору національної безпеки і оборони, банківського сектору, промисловості, транспорту, зв'язку, енергетики. Використання в таких системах у якості транспортної мережі глобальної мережі Інтернет або радіоканалів підвищує, як відомо, ризики погіршення їх гарантоздатності. В умовах кібератак це може привести до порушення в СОІ, як цілісності даних керування (руйнування, зловмисна підміна) внаслідок непередбачуваних змін системи та послуг, так і їх конфіденційності внаслідок отримання неавторизованого доступу до інформації про послуги в них. В свою чергу, це неодмінно призведе до суттєвого зростання ризиків втрат як для органів державного і військового управління, так й для суб'єктів господарювання державного і приватного секторів економіки й, як результат, взагалі може вивести сучасне суспільство на межу як локальних, так і глобальних техногенних катастроф. Проблеми забезпечення імітостійкості та конфіденційності таких систем ускладнюються низкою негативних чинників, а саме:

щорічним зростанням кількості реалізованих кібератак на СОІ, наслідком яких були значні фінансові та матеріальні збитки;

невизначеністю на законодавчому рівні особливостей захисту інформації (даних керування), що циркулює в СОІ;

нормативною неврегульованістю питання застосування технологій криптографічної переробки інформації для забезпечення імітостійкості та конфіденційності;

відсутністю вітчизняних розробок засобів криптографічного захисту інформації, що забезпечують швидкісне імітостійке шифрування.

Зважаючи на те, що в умовах зростання кількості та потужності кібератак суттєво ускладнюється вирішення завдання забезпечення імітостійкості та конфіденційності каналів передачі даних та/або команд управління (далі – інформації) в СОІ, як їх спроможності надавати послуги і сервіси, яким можна виправдано довіряти, внаслідок того, що саме вони зазнаватимуть найбільш руйнівних кібератак, та враховуючи, що в деяких випадках побудови СОІ, зокрема, в разі застосування мереж загального користування та радіоканалів, не існує більш дієвого механізму забезпечення конфіденційності та імітостійкості каналів передачі команд управління та даних, ніж технології криптографічного захисту інформації (КЗІ), **наукове завдання дисертаційної роботи** полягає у розробленні теоретичних і прикладних засад побудови та забезпечення методами криптографічної обробки інформації імітостійкості та конфіденційності даних в СОІ з урахуванням множини кіберзагроз та потенційно можливих наслідків їх реалізації. В цей час воно залишається невирішеним в повному обсязі й тому потребує свого розв'язання.

Дослідженню проблем забезпечення цілісності та конфіденційності данних в СОІ присвячені роботи A. Avizienis, В.С. Харченка, О.В. Федухіна, В.Л. Бурячка, В.Б. Дудікевіча, J.-C. Laprie, B Randell, C. Landwehr, I.E. Dobson, С.В. Зибіна, О.В.Копійки, О.М.Трофимчука, Д.В. Стефанишина, розв'язку задач імітостійкого шифрування, що не поширює помилок, присвячені роботи А.В. Бабаша, М.М. Глухова, І.Д. Горбенка, А.Ю. Зубова, В.М. Рудницького, В.О.

Устименка, Г.П. Шанкина, Shannon C.E., Diffie W., Hellman M. та багатьох інших. Особливість вирішення цих завдань обумовлюється різноманіттям методів побудови СОІ, відсутністю комплексного підходу до забезпечення коректного функціонування СОІ, а також наявністю невизначеностей, викликаних постійно змінними умовами функціонування таких систем. Зазначене, як результат, негативно впливає на загальний рівень імітостійкості та конфіденційності даних в СОІ. Зважаючи на таке, розробка моделей та методів забезпечення імітостійкості КЗІ в СОІ, визначених специфічними умовами функціонування, які за рахунок застосування імітостійкого шифрування, введення системи контролю правильності функціонування та блокування роботи каналу інформаційного обміну, дозволили б підвищити рівень імітостійкості і конфіденційності та запобігти несанкціонованим діям щодо інформації в СОІ, саме **й визначає актуальність теми дослідження**.

***Зв'язок роботи з науковими програмами, планами, темами.*** Дисертаційна робота пов'язана з вирішенням науково-технічних задач, сформульованих в Стратегії кібербезпеки України, затвердженої Указом Президента України №96/2016 від 27.01.2016 р., в Стратегії національної безпеки України, затвердженої Указом Президента України № 287/2015 від 26.05.2015 р., а також в «Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затвердженому Наказом №660 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02.12.2014 р. Частина завдань дисертаційної роботи вирішена автором в рамках науково-дослідної роботи (НДР) на тему «Базис-Наука» (номер державної реєстрації 0119U000042дс), яку виконано у Інституті проблем математичних машин і систем НАН України в 2020 році.

***Мета і завдання дослідження.*** Метою дисертаційної роботи є підвищення рівня імітостійкості та конфіденційності інформації в системах обробки інформації в умовах кібератак, за рахунок розробки й впровадження адекватних умовам застосування методів і моделей забезпечення надійного криптозахисту таких систем. Для досягнення поставленої мети в роботі необхідно розв'язати такі **завдання**:

1) дослідити множину актуальних загроз і уразливостей інформації, що циркулює в СОІ;
2) побудувати уточнені моделі порушника та загроз, а також автоматну модель безпеки функціонування каналів управління СОІ в умовах впливу кібератак;
3) розробити метод генерації потоку підстановок для шифру багатоалфавітної заміни (БАЗ) для забезпечення в СОІ конфіденційності та цілісності інформації;
4) розробити метод виявлення атак на програмні реалізації засобів КЗІ в СОІ;
5) розробити модель функціонування (криптосхему) шифратора БАЗ (модулю криптографічного захисту інформації) в СОІ;
6) вдосконалити метод оцінки ефективності застосування сучасних криптосистем.

Зважаючи на таке, ***об'єктом дослідження*** в роботі є процеси створення та використання нових моделей та методів забезпечення імітостійкості та конфіденційності КЗІ в СОІ. ***Предметом дослідження*** – моделі та методи для

забезпечення імітостійкості та конфіденційності даних в СОІ в умовах зростання потужності кібератак та ймовірності цільового ураження систем.

***Методи дослідження*.** При вирішенні поставлених задач в дисертаційній роботі було використано методи теорії ймовірностей та математичної статистики, математичного моделювання, синтезу та аналізу криптосистем.

***Наукова новизна одержаних результатів.*** Новими результатами, отриманими в дисертаційній роботі є:

1) вперше розроблений метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в СОІ, впровадження якого шляхом *реалізації двоступеневого критерію виявлення аномалій* дозволяє своєчасно виявити момент настання певної критичної ситуації та прийняти рішення щодо подальших дій;

2) вперше розроблена модель функціонування (криптосхема) шифратора БАЗ (модулю криптографічного захисту інформації) в СОІ, впровадження якої *за рахунок методу виявлення атак на програмні реалізації засобів криптографічного захисту інформації в СОІ та методу генерації потоку підстановок для шифру БАЗ* дозволяє забезпечити конфіденційність і цілісність інформації, що циркулює в СОІ, та в умовах кібератак підвищити функціональну безпеку та живучість самої системи;

3) вперше розроблений метод генерації потоку підстановок шифру багатоалфавітної заміни для забезпечення в СОІ конфіденційності та цілісності інформації, впровадження якого *за рахунок реалізації імітостійкого шифрування на основі оригінального швидкісного алгоритму формування потоку підстановок замін, критерію вибору степеню таких замін та процедури оцінки якості послідовності підстановок шифру багатоалфавітної заміни* дозволяє обрати таку степень підстановок, яка б забезпечувала достатню швидкодію криптоперетворення та була б раціональною для забезпечення захисту повідомлень від підробки;

4) удосконалений метод оцінки ефективності застосування криптосистем, на базі *врахування співвідношення середнього значення максимальних втрат власника СОІ у випадку успішних кібератак на систему захисту до мінімальної вартості реалізації таких атак*, що дозволило, на відміну від існуючих, визначити границі для відносної ефективності системи захисту інформації в СОІ в умовах реалізації кіберзагроз.

***Практичне значення одержаних результатів*** у сукупності складає підґрунтя для забезпечення імітостійкості та конфіденційності каналів передачі даних (команд управління) в СОІ.

Одержані результати дозволяють:

визначити границі для відносної ефективності системи захисту інформації в СОІ в умовах кібератак;

знизити ймовірність підробки команди управління до прийнятної для практичного застосування величини, що оцінується величиною $10^{-6}$;

знизити час на виявлення атаки приблизно на 20%;

знизити вартість системи виявлення атак на програмні реалізації засобів КЗІ приблизно на 25%.

Аналіз можливості застосування запропонованих моделей і методів забезпечення конфіденційності та імітостійкості даних було досліджено на прикладі дистанційно пілотованих літальних апаратів (ДПЛА), під час якого було з’ясовано, що їх застосування дає можливість своєчасного автоматичного прийняття рішення про його перехід в режим автономного виконання завдань в разі виявлення

реальних загроз штатному функціонуванню та можливості перехоплення каналу управління.

Отримані науково-практичні результати були перевірені за допомогою створеного в рамках роботи макету моделюючого комплексу інформаційної технології криптографічної обробки інформації. В ході імітаційного моделювання шифру БАЗ з достатньо високим рівнем надійності були підтверджені теоретичні розрахунки дослідження.

***Результати дисертаційних досліджень реалізовані й впроваджені в:***

Інституті проблем математичних машин і систем НАН України під час виконання НДР «Базис-Наука» (державний номер реєстрації 0119U000042дс) спрямованої на вирішення питань побудови мережі гарантоздатних ситуаційних центрів сектору безпеки і оборони (акт впровадження від 30.11.2020 р.).

Національному центрі управління та випробувань космічних засобів під час виконання НДР «Розробка науково-технічних пропозицій з організації віддаленого управління станціями оптико-електронних спостережень типу 1 та типу 2» (номер держ. реєстрації 0120U105420), що дозволило забезпечити цілісність та конфіденційність команд управління станціями оптико-електронних спостережень в режимі віддаленого доступу (акт впровадження від 30.11.2020 р.).

Київському університеті імені Бориса Грінченка в рамках навчальних дисциплін «Методи побудови та аналізу криптосистем», «Математичні методи криптографії» та впроваджені в програмно-апаратне забезпечення «Центру технологій захисту інформаційних активів» при розгортанні Лабораторії криптографічного та технічного захисту інформації (акт впровадження № 71-н від 30.11.2020 р.).

***Особистий внесок здобувача.*** Всі наукові результати, що виносяться на захист, одержано здобувачем самостійно. У роботах, написаних у співавторстві, здобувачеві належить: в [1] – профіль захищеності систем зв'язку, [2] – модель управління захистом інформації, [3] – формальна модель управління захистом інформації в інформаційно-телекомунікаційній системі; [4] – модель системи виявлення вторгнень; [5] – аналіз методів контролю захищеності корпоративних мереж, [6] – аналіз методів систем захисту персональних даних, [7] – алгоритм генерації підстановок заміни, [8] – криптосхема реалізації шифру БАЗ та блоку виявлення атак, [9] – застосування організаційних і технічних засобів захисту, [10] – модель утворення прихованих каналів, [11] – алгоритм управління правами доступу, [12] – модель порушника та метод оцінки безпеки бездротових систем розподілу; [13] – обгрунтування показників ефективності, часових ресурсів та витрат; [19] – формування вимог щодо гарантоздатності АСУ; [20] – модель порушника та реалізації кібератак, [21] – алгоритм вибору степеню підстановок.

***Апробація результатів дисертації.*** Основні положення і результати досліджень доповідалися та обговорювалися на I Міжнародній науково-технічній конференції «Актуальні проблеми розвитку науки і техніки» (м. Київ, ДУТ, 2015), II Міжнародній науково-технічній конференції «Актуальні проблеми розвитку науки і техніки» (м. Київ, ДУТ, 2015), III Міжнародній науково-технічній конференції «Актуальні проблеми розвитку науки і техніки» (м. Київ, ДУТ, 2016), Міжнародній науково-технічній конференції «Сучасні інформаційно-телекомунікаційні технології» (м. Київ, ДУТ, 2015), Міжнародній науково-технічній конференції студентства та молоді «Світ телекомунікацій та інформатизації» (м. Київ, ДУТ, 2015р.), II Всеукраїнській науково-практичній конференції «Кібербезпека в Україні:

правові та організаційні питання» (Одеса, 17 листопада 2017р.), IX Всеукраїнській науково-практичній конференції «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 30 березня 2018р), I Міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) (Київ, 5-6 квітня 2018 р.), VIII Міжнародній конференції «Математика. Інформаційні технології, Навчання (м. Львів, 2-4 червня 2019р.), Міжнародній конференції Cyber Hygiene ( 30 листопада 2019р).

***Публікації.*** За результатами дисертаційної роботи опублікована 21 наукова праця, 1 колективна монографія, 9 наукових статей, написаних у співавторстві й опублікованих у наукових спеціалізованих фахових виданнях України, 3 наукові праці, що входять до наукометричної бази SCOPUS. Разом з тим основні наукові результати додатково відображені у 9 тезах доповідей на семінарах та науково-практичних конференціях. Із праць, що опубліковано в співавторстві, у дисертаційній роботі використано виключно ті результати, які одержано здобувачем особисто.

***Обсяг і структура дисертації.*** Дисертаційна робота складається зі вступу, трьох розділів, висновків, додатків і списку використаних літературних джерел зі 120 найменувань та 3 додатки. Повний обсяг дисертації складає 150 сторінок машинописного тексту. Основний зміст викладений на 130 сторінці. Робота ілюстрована 25 рисунками та 14 таблицями.

## ОСНОВНИЙ ЗМІСТ

У **вступі** обґрунтовано актуальність теми, сформульовано мету і завдання досліджень, визначено наукову новизну та практичне значення роботи, наведено відомості про публікації, апробацію та впровадження результатів роботи.

**У першому розділі** перш за все проведено детальний аналіз та визначено особливості функціонування СОІ, вперше побудовано органіграму типових проблем забезпечення забезпечення імітостійкості та конфіденційності даних (рис. 1), а також визначено фактори які обумовлюють зростання складності забезпечення імітостійкості та конфіденційності СОІ.

Зокрема, з’ясовано, що на складність розв’язання проблем забезпечення імітостійкості та конфіденційності даних в СОІ суттєво впливають такі негативні тренди:

- слабка ефективність заходів щодо протидії кіберзагрозам, включаючи наукове забезпечення відповідних процесів;
- безсистемність заходів щодо захисту кіберпростору;
- недостатній рівень координації та взаємодії між суб’єктами забезпечення кібербезпеки, а також суспільством;
- невідповідність стану заходів щодо убезпечення електронних комунікацій рівню їх роз витку, невизначеність на законодавчомурівні статусу інформації, що циркулює у СОІ;
- недостатній розвиток організаційно-технічного забезпечення кібербезпеки, низька готовність певних служб забезпечити безпеку СОІ в умовах кібервпливу;
- низький рівень захищеності кіберпростору;
- недостатня увага рівню захищеності інформаційної інфраструктури СОІ.

Про останнє свідчить статистика сталого зростання кількості успішних атак у кіберпросторі та спроб несанкціонованого втручання в роботу СОІ, відсутність конкретних вимог та норм щодо технічного захисту інформації, що циркулює у СОІ та особливостей застосування засобів КЗІ, а також недосконаліть існуючої нормативно-правової бази, яка регламентує лише впровадження технологій та методів забезпечення безпеки переважно в тих СОІ, де обробляється інформація, щодо якої законодавчо визначена відповідальність тощо.


Рис. 1 Органіграма основних проблем забезпечення імітостійкості та конфіденційності даних в СОІ

На наступному кроці з урахуванням потенційних вразливостей СОІ у плані можливості непередбачуваних змін системи та послуг, що надаються (властивість цілісності), а також неавторизованого доступу до інформації про послуги (властивість конфіденційності), проведено аналіз факторів, що сприяють успішній реалізації атак та надано якісну оцінку ймовірності успішної реалізації атак для різних типів реалізації засобів захисту (програмних -- ПЗ, програмно-апаратних – ПАЗ, апаратних - АЗ) для визначених класів безпеки (табл.1).

Таблиця 1

Фактори що сприяють реалізації атак

| № | Фактори що сприяють реалізації атак (загрози) | Характеристика ймовірності успішної реалізації атак для різних типів реалізації засобів КЗІ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Класи безпеки ПЗ | | | Класи безпеки АПЗ | | | Класи безпеки АЗ | | |
| | | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 |
| 1. | Ненавмисні помилки операторів обслуговування | В | В | С | С | С | С | С | Н | Н |
| 2. | Несанкціоновані дії операторів безпеки (інсайдери), включаючи вхід до системи в обхід засобів захисту з метою забезпечення в подальшому доступу порушника. | В | В | В | В | С | С | С | С | Н |
| 3. | Збої та відмови технічних засобів та носіїв інформації | В | В | В | С | С | С | С | Н | Н |
| 4. | Навмисне пошкодження або крадіжка обладнання | В | В | В | С | С | С | С | Н | Н |
| 5. | Руйнування даних та команд, нав'язування хибної інформації у кінцевому обладнанні за допомогою спеціальних засобів. | В | В | В | С | С | С | С | С | Н |
| 6. | Відмова в обслуговуванні внаслідок впливу на канал управління | В | В | В | С | В | В | Н | С | Н |
| 7. | Збої та відмови програмного забезпечення внаслідок помилок етапу проектування | С | С | С | С | С | Н | Н | Н | Н |
| 8. | Некоректна інсталяція та конфігурування програмного забезпечення (ОС, прикладне програмне забезпечення) | В | В | В | С | С | С | С | С | С |
| 9. | Пошкодження файлів (у т.ч. системних журналів ОС) внаслідок зовнішніх випадкових факторів | Н | Н | Н | Н | Н | Н | Н | Н | Н |
| 10. | Ураження системи шкідливими кодами (вірусами) | В | В | В | В | С | С | С | Н | Н |
| 11. | Незаконне одержання паролів та інших реквізитів розмежування доступу з наступним маскуванням під зареєстрованого користувача | В | В | В | В | С | С | С | Н | Н |
| 12. | Несанкціоноване відключення засобів захисту | В | В | В | В | В | В | С | С | Н |
| 13. | Підбір та злам паролів | В | С | С | С | С | С | С | С | Н |

Надалі було проведено порівняльний аналіз методів контролю цілісності, протидії маніпулюванню даними в СОІ (табл. 2) і забезпечення їх конфіденційності (табл. 3), а також визначено функціональні і експлуатаційні переваги та недоліки реалізації криптографічних перетворень у вигляді програмних (ПЗ), програмно-апаратних (ПАЗ) та апаратних (АЗ) засобів (табл. 4).

Таблиця 2

Порівняльний аналіз методів протидії маніпулюванню даними та/ або контролю цілісності

| Метод | | Переваги | Недоліки | Ранг |
|---|---|---|---|---|
| 1 | Електронний цифровий підпис (ЕЦП) | Практично неможливо підробити ЕЦП, що побудоване на основі сучасних алгоритмів.<br>Дозволяє будувати системи з юридично значущим доведенням авторства повідомлення. | Відносно тривалий час формування та перевіряння ЕЦП.<br>ЕЦП для коротких повідомлень може мати довжину, що перевищує їх розмір на два порядки.<br>Для захисту конфіденційності за допомогою симетричних шифрів потрібно мати три ключі: секретний для шифрування, секретний для формування ЕЦП та відкритий для його перевірки.<br>Потребує наявності в системі третьої сторони – центру сертифікації ключів. | III |
| 2 | Коди автентифікації повідомлень (МАС) | Перевірка цілісності інформації за допомогою лише секретного ключу.<br>Мала ймовірність підробки МАС, що не перевищує величини $2^{-m}$, де $m$ – довжина МАС | У випадку забезпечення конфіденційності повідомлень за допомогою симетричних БШ потрібно мати два ключі: шифрування та формування МАС;<br>Генерація МАС за допомогою алгоритму блокового шифрування потребує значного часу. | II |
| 3 | Використання позначок часу. | Не суттєво збільшує довжину повідомлення.<br>Не потребує суттєвих витрат часу процесора. | Потребує шифрування повідомлень та процедури синхронізації годинників приймача та передавача;<br>Для забезпечення низької ймовірності підробки потрібна велика розрядність цифрового годинника. | IV |
| 4 | Зміна ключів за «плаваючим» графіком. | Не змінює швидкості виробничої потужності системи. | Не суттєво підвищує імітостійкість;<br>Ускладнює процедури управління ключами. | V |
| 5 | Імітостійке шифрування. | Має значно більшу швидкодію серед інших криптографічних методів захисту.<br>Не втрачає стійкості в разі повторення ключу шифрування. | Генерація псевдовипадкової послідовності (ПВП) підстановок заміни: $X_1$, $X_2$, ..., $X_m$, .... потребує певного часу, що зменшує пропускну здатність;<br>Відмова блоку генерації ПВП внаслідок несанкціонованого втручання у роботу системи може зруйнувати систему безпеки. | I |

Таблиця 3

Порівняльний аналіз криптографічних методів забезпечення конфіденційності

| Криптографічне перетворення | Переваги | Недоліки |
|---|---|---|
| Блокове шифрування | Забезпечує імітостійке шифрування в режимі СВС.<br>Достатньо складні співвідношення між вихідним і шифрованим текстом для того, щоб аналітичні і (або) статистичні методи визначення вихідного тексту і (або) ключа на основі відповідності вихідного і шифрованого тексту були б по можливості такими, що не реалізуються. | Викривлення одного біту в зашифрованому блоці призводить до викривлення всього блоку у режимі шифрування ЕСВ, або залишкової частини шифротексту в режимі СВС,що вимагає додаткового застосування потужних кодів виправляють помилки. З двох однакових блоків вихідного тексту виходять однакові блоки шифрованого, що підвищує ризики підробки відповідних повідомлень. |
| Потокове шифрування | Висока швидкість шифрування та розшифрування<br>Потік ключів генерується з короткого основного ключа за допомогою однозначних певних детермінованих алгоритмів. | Практична реалізація «наддовгих» ключових послідовностей і їх зберігання занадто важке і незручне. Вставка або випадання одного двійкового символу в шифрограмі призводить до неправильного розшифрування інших символів через втрату синхронізації. Число параметрів, що впливають на їх стійкість, істотно більше, ніж для блокових шифрів |

Таблиця 4

Порівняльна таблиця властивостей реалізації засобів КЗІ

| Тип реалізації | Переваги | Недоліки |
|---|---|---|
| ПЗ | 1. Низька вартість засобу<br>2. Гнучкість | 1. Слабка захищеність від атак на реалізацію<br>2. Невисока продуктивність |
| ПАЗ | 1. Підвищений рівень безпеки<br>2. Підвищена продуктивність | 1. Середній рівень захисту від атак на реалізацію<br>2. Підвищена вартість |
| АЗ | 1. Висока продуктивність<br>2. Відомі механізми блокування побічних каналів витоку | 1. Надто висока вартість<br>2. Орієнтованість на конкретні протоколи |

На основі аналізу сучасних підходів щодо вирішення завдань гарантоздатності у частині імітостійкості та конфіденційності в розділі констатовано, що універсального науково-методичного апарату, який дозволив би вирішити ці завдання на практиці нажаль не існує. Зважаючи на те, що прийняття адекватних мір та проведення обґрунтованих заходів із забезпечення імітостійкості та конфіденційності даних в СОІ не повинно суттєво впливати на виконання нею функціональних завдань за призначенням та суттєво уповільнювати її швидкодію, реалізація засобів захисту повинна узгоджуватися з загальною архітектурою системи, а їх працездатність має належним чином контролюватися. Таким чином за результатами виконання першого розділу було обрано напрям дослідження, що ґрунтується на необхідності вдосконалення побудови програмних засобів імітостійкого шифрування та розробці нових, ефективних методів і моделей виявлення атак на програмні реалізації системи інформаційної безпеки СОІ, сформовано завдання та побудовано структурно-логічну схему дослідження (рис. 2).

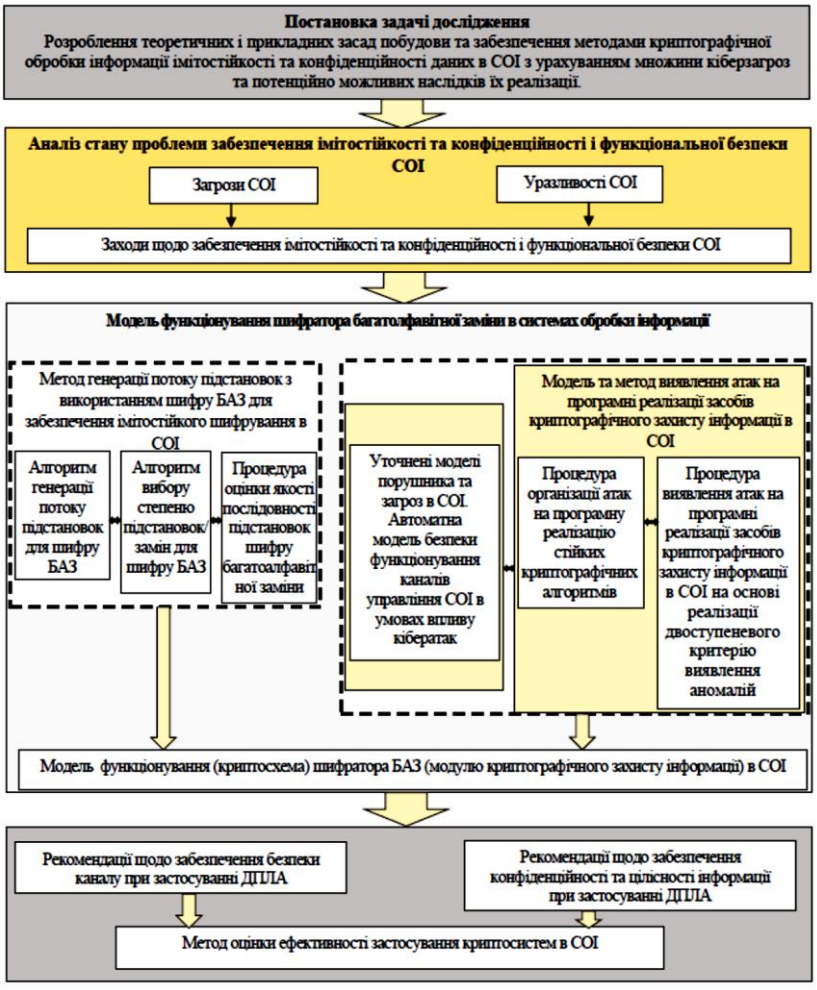


Рис.2. Структурно-логічна схема проведення дослідження

**У другому розділі,** виходячи з переваг у разі застосування в СОІ для забезпечення конфіденційності та цілісності інформації імітостійкого шифрування, а також, враховуючи, що відомі підходи до формування послідовностей випадкових і псевдовипадкових підстановок заміни мають певні недоліки (складність реалізації

методу формування підстановки багаторазового добутку підстановок з деякої їх множини, низька швидкодія методу безповторного набору підстановок тощо), сформовано модель функціонування шифратора БАЗ в СОІ. Її базовими складовими є метод генерації потоку підстановок для шифру БАЗ для забезпечення імітостійкого шифрування в СОІ та метод контролю стану конфіденційності програмних реалізацій засобів КЗІ в СОІ.

***Метод генерації потоку підстановок для шифру БАЗ з метою забезпечення імітостійкого шифрування в*** СОІ в свою чергу ґрунтується на вирішенні задачі швидкого формування підстановок з симетричної групи підстановок $S_n$. Суть методу полягає у формуванні нижнього рядка підстановки заміни в безповторному наборі підстановок із випадкової (або псевдовипадкової) рівномірно розподіленої послідовності (РРВП). Для цього використовується потік випадкових чисел $j_0, j_1, \dots, j_m, \dots \in \mathbb{Z}_n$ таким чином, що символ, який присутній у сформованій частині рядка, відхиляється та у подальшому не використовується. Таким чином процес може продовжуватися досить довго.

Оскільки результатом вибірки з РРВП є також РРВП, то тільки частина «відрізків» $(j_0, j_1, \dots, j_{n-1})$ без корегування може утворювати нижчий рядок підстановки. Зважаючи на таке ймовірність отримання підстановки без корегування дорівнює:

$$\pi_n = P\left(\begin{pmatrix} 0 & \dots & n-1 \\ j_0 & \dots & j_{n-1} \end{pmatrix} \in S_n\right) = \frac{|S_n|}{n^n} = \frac{n!}{n^n}. . \quad (1)$$

Для оцінки ймовірності у формулі (1) можливо скористатися формулою Стірлінга для оцінки факторіала:

$$n! = \sqrt{2\pi n} \cdot n^n \cdot e^{-n}\big(1 + o(1)\big), \text{ де } o(1) \to 0 \text{ при } n \to \infty.$$

Звідки отримуємо оцінку для вказаної ймовірності:

$$\pi_n = \frac{\sqrt{2\pi n} \cdot n^n \cdot e^{-n}}{n^n} = \sqrt{2\pi n} \cdot e^{-n} \quad . \quad (2)$$

Оскільки обсяг вихідних випадкових даних, що необхідні для формування однієї підстановки, асимптотично оцінюється величиною $C \cdot n \cdot \ln n$, де $C$ – деяка константа, - практичне застосування цього методу для побудови швидкісних систем управління є проблематичним. З метою усунення цієї проблеми в роботі запропоновано підхід, що полягає у розробці нового швидкісного алгоритму генерації потоку підстановок для шифру БАЗ, впровадження якого забезпечуватиме конфіденційність та імітостійкість інформаційного обміну в СОІ.

Для опису алгоритму генерації в роботі доведено такі твердження.

**Твердження 1.** Якщо найбільший спільний дільник чисел $n, l \in \mathbb{N}, n > 1$: $(n, l) = 1$ , то для фіксованого $\forall \delta \in \mathbb{Z}_n$ у рівнянні

$$\delta + k \cdot l = x_k \bmod n, \quad (3)$$

для різних $k \in \mathbb{Z}_n$ усі значення $x_k \in \mathbb{Z}_n$ різні.

Дійсно, нехай $k_1 \neq k_2$, але $x_1 = x_2$. Тоді з рівняння (3) маємо: $\delta + k_1 \cdot l = \delta + k_2 \cdot l \bmod n$, або $(k_1 - k_2) \cdot l = 0 \bmod n$. Останнє суперечить вимозі взаємної простоти чисел $(n, l) = 1$, з цього випливає $\forall k_1 \neq k_2 \implies x_1 \neq x_2$, що й потрібно було довести.

Сформулюємо зміст розробленого алгоритм генерації підстановки степені $n$: $X = \begin{pmatrix} 0 & \dots & n-1 \\ x_0 & \dots & x_{n-1} \end{pmatrix}$ за допомогою послідовності випадкових чисел $j_0, j_1, \dots, j_m, \dots \in \mathbb{Z}_n$.

Для формального опису алгоритму скористаємось оператором Бекуса присвоювання значення деякої змінної «:=». На кожному кроці алгоритму визначається один перехід у підстановці $\begin{pmatrix} k \\ x_k \end{pmatrix}$, позначимо через $\mathcal{A}$ множину переходів, що сформовані.

Тоді формалізований опис послідовності кроків виконання алгоритму генерації потоку підстановок у випадку $(l = 1, \delta)$ буде мати вигляд, що наведений в табл. 5, а його блок схема генерації однієї підстановки у позначеннях ЕСКД наведена на рис. 3.

Таблиця 5

Формалізований опис методу генерації потоку підстановок $(l = 1, \delta)$

| Крок | Формалізований опис | Коментар |
|---|---|---|
| 0. | $t := 0$. | $t$ - початок поточного вектору РРВП. |
| 1. | $k := j_t, m := t + 1,\ \mathcal{A} := \{\emptyset\}$. | $k$ - номер переходу; $m$ - номер кроку підстановки. |
| 2. | $x_k := j_m$. | Визначення значення для нижнього рядка $\begin{pmatrix} k \\ x_k \end{pmatrix}$. |
| 3. | $\mathcal{A} := \mathcal{A} \cup \{x_k\}$. | Доповнюємо множину вже визначених переходів. |
| 4. | $k := k + 1 \bmod n$. | Збільшуємо номер позиції у верхньому рядку для формування наступного переходу. |
| 5. | $m := m + 1$. | Номер чергового випадкового числа. |
| 6. | Якщо $m = n - 1$, то виконуємо крок 10, якщо НІ – виконуємо крок 7. | Умовний перехід на завершення підстановки. |
| 7. | Якщо має місце $j_m \notin \mathcal{A}$ - виконуємо крок 2, якщо НІ – виконуємо наступний крок 8. | Умовний перехід до способу обчислення наступного значення для нижнього рядка. |
| 8. | $j_m := j_m + \delta \bmod n$. | Модифікація випадкового числа. |
| 9. | Далі виконуємо крок 7 | Перехід до перевірки у полі визначених переходів. |
| 10. | Останньому переходу присвоюємо значення $x_{n-1} := \mathbb{Z}_n \setminus \mathcal{A}$. | Завершення формування підстановки;. |
| 11. | Чи існує ще нешифрований символ? Якщо ТАК – виконуємо крок 12, якщо НІ – завершуємо | Перевірка вхідного потоку відкритих символів |
| 12. | $t := t + n$. | Початок чергового вектору. |
| 13. | Перехід до кроку 1. | Перехід до початку формування нової підстановки. |

Виходячи з **твердження 1** легко зрозуміти коректність роботи запропонованого алгоритму у розумінні генерації множини підстановок, елементи якої співпадають з елементами симетричної групи $S_n$.

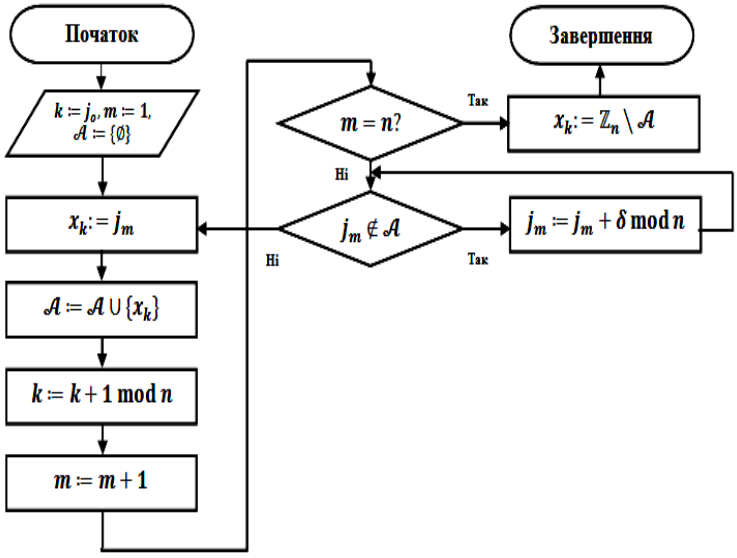


Рис.3. Блок-схема алгоритму генерації підстановок

Важливою характеристикою схеми генерації підстановок з точки зору забезпечення необхідних криптографічних якостей шифру багатоалфавітної заміни є: кількість підстановок, що генеруються; ймовірності їх зустрічаємості та матриця перехідних ймовірностей.

**Твердження 2**. Якщо послідовність випадкових чисел $j_0, j_1, \dots, j_{n-1} \in \mathbb{Z}_n$ є незалежною у сукупності та має рівномірний розподіл, тоді алгоритм генерації

підстановок забезпечує формування $S_n$ - симетричної групи підстановок степені $n$. Цей висновок є достатньо зрозумілим, оскільки в умовах твердження ймовірність появи будь-якої послідовності $j_0, j_1, \dots, j_{n-1} \in \mathbb{Z}_n$ :

$$P(j_0, j_1, \dots, j_{n-1} \in \mathbb{Z}_n) = n^{-n} \neq 0,$$

у тому числі такої, що утворює нижній рядок підстановки без коригування послідовності. Таким, чином за допомогою цього алгоритму може бути генерована будь яка підстановка з $S_n$ - симетричної групи підстановок степеня $n$.

З метою підвищення криптографічної стійкості шифру БАЗ в роботі було розроблено алгоритм вибору степеню підстановок/замін шифру БАЗ для забезпечення захисту повідомлень від підробки. Для цього було доведено такі твердження.

**Твердження 3.** У випадку практичної криптографічної стійкості шифру та джерела повідомлень без пам'яті для ймовірності $p_n$ підміни в каналі зв'язку шифрованого повідомлення довжини $L$ справедлива оцінка знизу:

$$p_n \geq 2^{-(1-H_0)L}. \quad (4)$$

У випадку $\mathrm{L} \geq 12$ біт ймовірність підміни в каналі зв'язку для більшості значень має більш придатні для практичного застосування значення $0{,}0006 \leq \mathrm{p_п} \leq 0{,}0359$.

**Твердження 4.** В випадку практично стійкого шифру багато алфавітної заміни з підстановками степеню $n$ для ймовірності $q_{rn}$ підміни в каналі зв'язку істинного повідомлення $M = (m_1, m_2, \dots, m_l)$ на фіктивне $\widetilde{M} = (\widetilde{m}_1, \widetilde{m}_2, \dots, \widetilde{m}_l)$ таке, що $M$ та $\widetilde{M}$ відрізняються лише на $r$ місцях, справедлива оцінка:

$$q_{rn} = (n-1)^{-r}. \quad (5)$$

При цьому ймовірність вгадування порушником $r$ символів з першого разу, яка може слугувати оцінкою для рівня імітостійкості шифру багатоалфавітної заміни, дорівнюватиме $q_{rn} = C_n^{-1} = (n-1)^{-r}$.

Для перевірки послідовності підстановок шифру багатоалфавітної заміни та оцінки їх якості в роботі було розроблено відповідну процедуру, суть якої полягає у використанні статистичного аналогу матриці перехідних ймовірностей $\mathcal{P}$, що обчислюється за формулою:

$$\mathcal{P} = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} = \sum_{X_i \in S_n} p_{X_i} \cdot \bar{X}_i, \quad (6)$$

де $p_{ij} = P(j/i),\ i, j \in \{\overline{1,n}\}$ - умовна ймовірність появи на виході вузла знаку $j$ в разі надходження знаку $i$; $\bar{X}_i$ – підстановочна матриця, що відповідає генерованій підстановці $X_i \in S_n$, $p_{X_i}$ – ймовірність генерації підстановки $X_i$.

При цьому перший визначений перехід $\binom{j_0}{j_1}$ з ймовірністю $1/n^2$ може приймати будь-яке значення із множини:

$$\mathcal{R} = \left\{\binom{0}{0}, \dots, \binom{0}{n-1}, \binom{1}{0}, \dots, \binom{1}{n-1}, \dots, \binom{n-1}{0}, \dots, \binom{n-1}{n-1}\right\},$$

На другому кроці починається розгалужений процес, який передбачає, що:

<u>*по-перше*</u>, з ймовірністю $(n-1) \cdot n^{-1}$ будуть отримані переходи $\begin{pmatrix} j_0 & j_0+1 \\ j_1 & j_2 \end{pmatrix}$, якщо випадкове число $j_2$ не співпадає з раніше отриманим числом $j_1$;

*по-другe*, з ймовірністю $n^{-1}$ будуть отримані переходи $\binom{j_0\ j_0+1}{j_1\ j_1+\delta}$, якщо випадкове число $j_2$ співпадає з раніше отриманим числом $j_1$.

Перший варіант формування нового переходу назвемо не модифікованим, інший модифікованим. Тоді метод формування підстановки можливо подати у вигляді процесу, зображеного на рисунку 4 й стверджувати, що розгалуження процесу створення підстановки відбувається з певною ймовірністю після кожного його кроку. При цьому для зручної реалізації алгоритму доцільно обирати значення, які відповідають розрядній сітці мікропроцесорів, а саме: $n = 2^m$, де $m = 2,4,8,\ldots$ При цьому коефіцієнт імітостійкості БАЗ для $n = 2^2$ є найменшим, а застосування $n = 2^8 = 256$ призведе до суттєвого уповільнення процесу шифрування порівняно з варіантом $n = 2^4 = 16$ (табл.6).

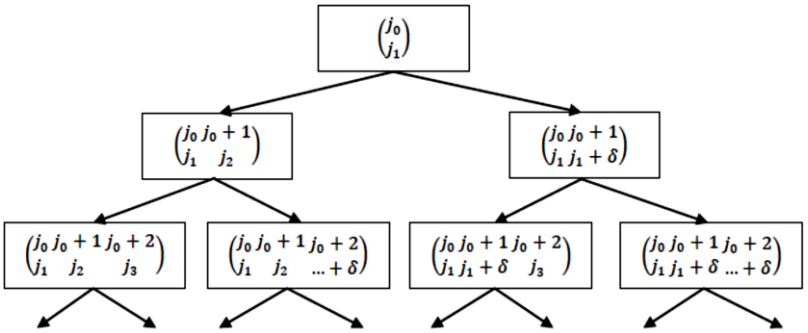


Рис.4. Схема процесу створення підстановки

Таблиця 6

Розрахункові характеристики методу генерації потоку підстановок з використанням шифру БАЗ для забезпечення імітостійкого шифрування в АСУ ОКІ

| № | Характеристики методу | | Степінь підстановки | | |
|---|---|---|---|---|---|
| | | | 4 | 16 | 256 |
| 1. | $q_{1п}$ | Імовірність підробки 1 символу | 0.333 | 0.067 | 0.008 |
| 2. | N | Стійкість при повторі ключа | 2 | 8 | 128 |
| 3. | S | Швидкодія порівняно з МБН (%) | 138.6 | 277.2 | 554.5 |
| 4. | V | Обсяг двійкової РРВП для генерації однієї підстановки (біт) | 8 | 64 | 4096 |

Як результат, застосування методу генерації потоку підстановок з використанням шифру БАЗ для забезпечення імітостійкого шифрування в СОІ (*шифру багатоалфавітної заміни на основі оригінального швидкісного алгоритму формування підстановок замін*) дозволить підвищити надійність захисту інформації в СОІ, а також знизити ймовірність підробки команди управління до прийнятної для практичного застосування величини порядку $10^{-6}$.

Наступним кроком у реалізації другого розділу дисертаційної роботи стало ***розроблення моделі та методу виявлення атак на програмні реалізації засобів КЗІ в СОІ.*** Підставою цьому є вимоги нормативних документів системи КЗІ щодо необхідності забезпечення контролю цілісності програмного коду, виявлення збоїв засобів захисту та помилок операторів. Метод ґрунтується на уточнених моделях порушника і загроз, а також автоматній моделі безпеки функціонування каналів управління СОІ в умовах впливу кібератак та полягає у дослідженні статистики аномальної поведінки (стану) засобу КЗІ та зводиться до виявлення зміни математичного сподівання в деякій новій випадковій послідовності, сформованій з вихідної.

При розробці моделі було зроблено припущення, що у випадку штатного функціонування СОІ деякий потік вимірюваних даних від об’єкту контролю є стаціонарним, а після настання деякої події він змінює розподіл своїх значень. Необхідно максимально точно виявити момент настання цій ситуації та

прийняти рішення щодо аномальності ситуації. Формалізуємо дану задачу в декілька кроків.

*Крок перший*. Нехай стосовно випадкової послідовності, що аналізується, $X = \{x_t, x_t \in R,\ t = \overline{1,N}\}$ розглядаються дві складні гіпотези: $H_0$: послідовність $X$ є стаціонарною з єдиною функцією розподілу ймовірностей, $H_1$: послідовністю $X$ є конкатенацією (результатом «склеювання») двох стаціонарних випадкових послідовностей з різними функціями розподілу:

$$X = X_1||X_2, \text{ де } X_1 = \{x_t, t = \overline{1,n^*}\},\ X_2 = \{x_t, t = \overline{n^*+1,N}\},\ n^* = [\theta N],\ 0 < \theta < 1. \quad (7)$$

Потрібно оцінити точку «склейки» n*.

Вважається, що послідовності $X_1$ і $X_2$ відрізняються між собою однією з двовимірних функцій розподілу, а саме, розподілу ймовірностей вектору $(x_t, x_{t+2})$:

$$F(u_0, u_1) = P\{x_t \le u_0, x_{t+2} \le u_1\} \quad (8)$$

до моменту $t_1^* = n^* - 2$ включно дорівнює F1(u), а при $t \ge t_2^* = n^* + 1$ дорівнює F2(u), причому

$$||F_1(u) - F_2(u)|| \ge \varepsilon > 0, \text{ де } ||\ldots|| \text{ - звичайна sup-норма.} \quad (9)$$

Відомо, що функція розподілу скінченновимірного випадкового вектора може бути наближена рівномірно з будь-якою точністю функцією розподілу ймовірностей випадкового вектора з скінченним числом значень. Звідси випливає, що якщо подати множину $R$ у вигляді об'єднання досить великої кількості областей $\{Aj,\ j = \overline{1,r}\}$, що не перетинаються $A_i \cap A_j = \emptyset$ для $i \ne j$, то вектор $(x_t, x_{t+2})$ можна апроксимувати по розподілу вектором з кінцевим числом значень. Тому, якщо ввести нові випадкові послідовності

$$V_t^{ij} = I\big(x_t \in A_i, x_{t+2} \in A_j\big),\ \text{де } 1 \le i \le r, 1 \le j \le r, \quad (10)$$

де I(A) - індикатор множини A, то хоча б в одній з них відбувається зміна математичного сподівання.

Отже, якщо скористатися алгоритмом, який виявляє зміну математичного сподівання, то цей же алгоритм виявить і зміну функції розподілу. Ця обставина дозволила в роботі обмежитися розробкою лише одного, базового алгоритму, який може виявляти зміну математичного сподівання. Для цього з метою виявлення моментів "розладнань" запропоновано сімейство статистик виду:

$$Y_N(n, \delta) = \left[\frac{n}{N}\left(1 - \frac{n}{N}\right)\right]^{\delta} \cdot \left[\frac{1}{n}\sum_{k=1}^{n} x_k - \frac{1}{N-n}\sum_{k=n+1}^{N} x_k\right], \quad (11)$$

де $0 < \delta \le 1,\ 1 \le n \le N-1,\ X = \{x_k,\ k = \overline{1,N}\}$ – послідовність, що досліджується.

Наведене сімейство статистик у випадку фіксованого $n$ є узагальненим варіантом статистики Колмогорова - Смірнова, що використовується для перевірки гіпотез збігу або відмінності функцій розподілу у двох вибірках. В роботі також доведено, що статистика виду (11) в разі $\delta = 1$ при $N \to \infty$ та збереженні співвідношення між обсягами "склеєних" реалізацій мінімізує максимально можливу ймовірність помилки оцінювання моменту «розладнання» (мінімаксна по порядку). При цьому:

$$P\{\max_{1\le n\le N-1}\sqrt{N}|Y_N(n,1)| > C^{(1)}\} \to 2\sum_{k=1}^{\infty}(-1)^{k+1}\exp(-2k^2\left(\frac{C^{(1)}}{\sigma_*}\right)^2) \equiv f(C^{(1)}), \quad (12)$$

де параметр $\sigma_*$ є стандартним відхиленням, *C(1)* – границя критерію, перевищення якої буде сприйматися, як виникнення «розладнання», значення $n_*$, для якого це
відбулося, є шуканим моментом «розладнання».

*Крок другий.* Зафіксувавши рівень ймовірності α «помилкової тривоги» про розладнання, під час статистичної обробки реальних даних визначимо рівень порога першого рівня $C^{(1)}$:

$$\alpha = f\left(C^{(1)}\sqrt{N}/\bar{\sigma_*}\right), \quad (13)$$

де $\bar{\sigma_*}$ є оцінкою параметра $\sigma_*$ (стандартне відхилення), а N є обсягом вибірки - послідовності, що досліджується.

У випадку гіпотези $H_1$ про подання вихідної послідовності вимірювань у вигляді конкатенації декількох стаціонарних випадкових послідовностей з різними функціями розподілу ймовірностей, застосуємо критерій припустимої кількості спрацювань («розладнань») Z. Тобто, вважаємо що має місце наступне рівняння:

$$n_1 + n_2 + \ldots + n_Z = N, \text{де } 2 \le Z < N - 2. \quad (14)$$

Для невеликої кількості послідовностей з метою визначення границі критерію можна скористатися нерівністю Чебишова: якщо випадкова величина Z має математичне сподівання μ та стандартне відхилення σ для заданого $\varepsilon > 0$:

$$P\{|Z-\mu| \ge \varepsilon\} \le \frac{\sigma^2}{\varepsilon^2}. \quad (15)$$

Якщо Z є випадковою величиною з одномодальним розподілом ймовірностей з математичним сподіванням μ та стандартним відхиленням $0 < \sigma < \infty$, то для будь якого $\lambda > \sqrt{8/3} \approx 1.63299\ldots$, має місце нерівність Височанського – Петунина, що покращує оцінку ймовірності відхилення:

$$P\{|Z-\mu| \ge \lambda\sigma\} \le \frac{4}{9\lambda^2}. \quad (16)$$

Зокрема, для типового відхилення у $3\sigma$ (три сигма) рівень значущості критерію - ймовірність "помилкової тривоги" обчислюється як: $\alpha = \frac{4}{9\lambda^2} \approx 0.0494$. Більш точний результат можливо отримати для випадку випадкової величини Z, що є сумою досить великої кількості незалежних випадкових величин $(m \to \infty)$: $Z = z_1 + z_2 + \ldots + z_m$.

Згідно інтегральної граничної теореми ймовірність відхилення можливо апроксимувати за допомогою функції нормального розподілу ймовірностей $N(0,1)$:

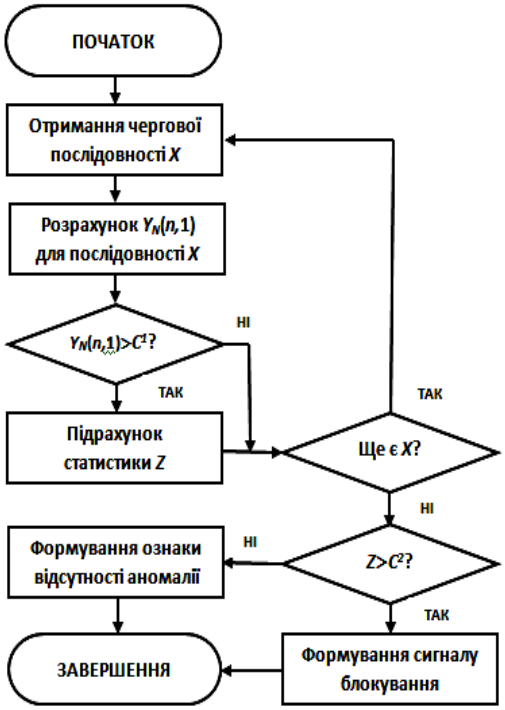


Рис. 5. Блок – схема алгоритму реалізації двоступеневого критерію виявлення аномалії у поведінці засобу КЗІ

$$P\left\{\left|\frac{Z-\mu}{\sigma}\right| \geq t_{1-\alpha}\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t_{1-\alpha}} \exp(-\frac{t^2}{2})dt \qquad .(17)$$

На підставі (14) розраховуємо границю критерію другого рівня: $C^{(2)} = \mu + t_{1-\alpha}\sigma$ Алгоритм обчислення критерію приведено на рис.5.

Як результат, застосування моделі та методу виявлення атак на програмні реалізації засобів КЗІ в СОІ дозволяє виявити момент настання певної критичної ситуації та прийняти рішення щодо її аномальності, відновити секретний ключ, за допомогою якого створені зашифровані повідомлення та/або розкрити вихідне значення зашифрованої інформації в СОІ, а також знизити вартість системи виявлення атак на програмні реалізації засобів КЗІ приблизно на 25%.

З метою забезпечення конфіденційності та цілісності інформації при прийомі та передачі в СОІ на третьому кроці другого розділу дистертаціної роботи було побудовано ***модель функціонування (криптосхему) шифратора БАЗ (модулю КЗІ)***. Модель включає генератор ПВП, алгоритм генерації підстановок заміни, систему контролю і блокування та вузол шифрування (рис. 6). Базою для моделі стали модель та метод виявлення атак на програмні реалізації засобів КЗІ в СОІ та методу генерації потоку підстановок з використанням шифру БАЗ. Її квінтесенція полягає в тому, що вона передбачає:

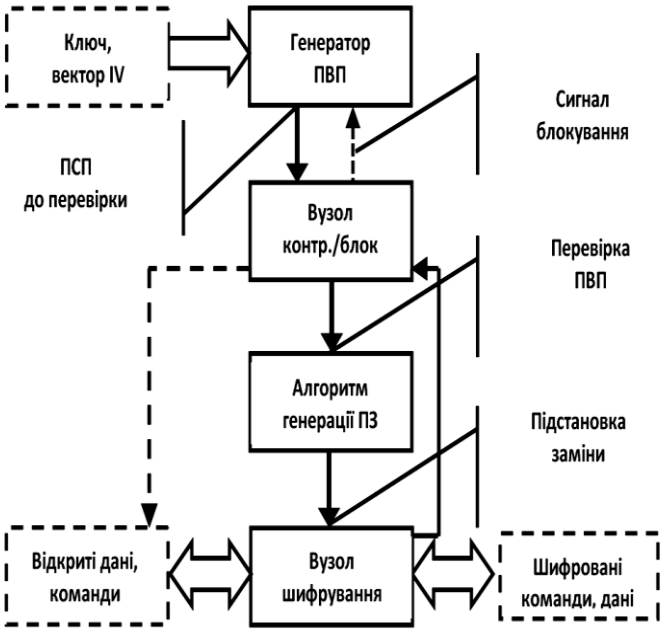


Рис. 6. Модель функціонування шифратора БАЗ

*по-перше*, при ініціалізації ключа – генерацію ПВП у відповідному блоці;

*по-друге*, перевірку правильності роботи генератора ПВП у блоці «Вузол контролю та блокування»;

*по-третє*, подачу ПВП сигналу блокування при збої генератора ПВП та його зупинку до відновлення правильної роботи;

*по-четверте*, при позитивному проходженні перевірки ПВП: – початок роботи алгоритму генерації підстановок заміни з подальшим шифруванням даних; – перевірку в блоці «Вузол контролю та блокування».

Впровадження зазначеної моделі дозволяє, на відміну від існуючих, забезпечити конфіденційність і цілісність інформації, що циркулює в СОІ та в умовах кібератак забезпечити власне функціональну безпеку і живучість самої системи.

**Третій розділ** присвячено дослідженню особливостей застосування запропонованих моделей і методів забезпечення імітостійкості та конфіденційності програмних реалізацій засобів для гарантованого керування дистанційно пілотованих літальних апаратів.

З цією метою в розділі описано алгоритм реагування ДПЛА на дії порушника та сформовано як рекомендації щодо забезпечення безпеки каналу та інформаційного

обміну з ДПЛА від активних і пасивних атак, так й рекомендації щодо забезпечення захисту інформації від несанкціонованого доступу до її смислового змісту. Проведено порівняння систем зв'язку Lightbridge 2 та OcuSync 2.0, що застосовуються у більшості сучасних ДПЛА та використовуваних систем шифрування AES (Advanced Encryption Standard) і 3DES (відомий як Triple DES - Data Encryption Standard) й зроблено такі висновки: 3DES використовує ідентичне шифрування DES, тоді як AES використовує абсолютно інше; 3DES має більш короткі та слабкі ключі шифрування порівняно з AES; 3DES використовує повторювані ключі шифрування, тоді як AES цього не робить; 3DES також використовує меншу довжину блоку порівняно з AES; шифрування 3DES займає більше часу, ніж шифрування AES. Застосування кожної з наведених систем шифрування не гарантує надійного криптозахисту. Тому на ДПЛА останнім часом все частіше встановлюють додаткове шифрувальне обладнання. Воно, в свою чергу, обтяжує квадрокоптер й може привести до несвоєчасного отримання ним керуючого сигналу. Це вимагає спрощення методів шифрування так, щоб ефективність забезпечення імітостійкості та конфіденційності повідомлень не зменшилась.

В дисертаційній роботі ця задача вирішується за рахунок застосування моделі функціонування шифратора БАЗ (рис.6), що забезпечує імітостійкість та конфіденційність даних в СОІ. Мета експериментальної апробації зазначеної моделі полягала в перевірці працездатності моделей і методів, що її утворюють та коректності використаного в них математичного апарату, а також правильності висновків про доцільність їх застосування. Результати обчислення часу на виконання задач кодування та/або декодування інформації, отримані при застосуванні криптосхеми подано в табл.7.

**Таблиця 7**

**Середній час тестів для криптографічних перетворень**

| Вид тестування | Результати |
|---|---|
| Швидкість виконання шифрування (сек) | 0,215 с |
| Швидкість виконання дешифрування (сек) | 0,219 с |
| Частотність (%) | 13% |
| Актуальність переданої інформації | 58 с |
| Криптостійкість | 6 днів |

З метою практичної перевірки моделей і методів, розроблених в ході дисертаційного дослідження, а саме якості методу генерації потоку підстановок з використанням шифру БАЗ для забезпечення імітостійкого шифрування в СОІ та модель функціонування шифратора БАЗ на мові Java було створено макет моделюючого комплексу інформаційної технології криптографічної обробки інформації (МК ІТ КОІ). Логічну схему макету наведено на рис 7.

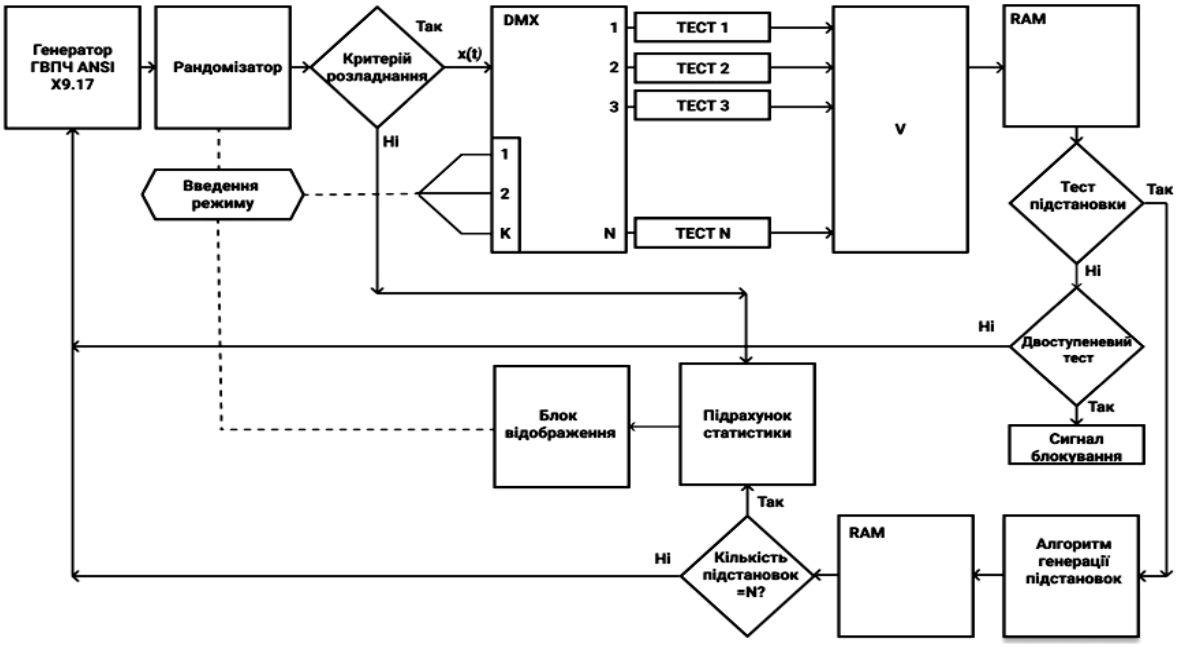


Рис. 7. Логічна схема макету моделюючого комплексу інформаційної технології криптографічної обробки інформації в СОІ

Комплекс забезпечує генерацію двійкових випадкових даних, їх рандомізацію відповідно до заданого режиму, вибір схеми тестування, генерацію заданої кількості підстановок визначеного розміру та відображення отриманих результатів за заданою діаграмою. Панель управління зазначеного комплексу, яку наведено на рис. 8, відображає заданий режим генерації кількості підстановок N = 5000, розміру m = 16 з двійкової послідовності з імовірністю зустрічаємості P(1) = 0,5001. Для перевірки використано критерій Пірсона $\chi^2$, вид діаграми - кільцева.

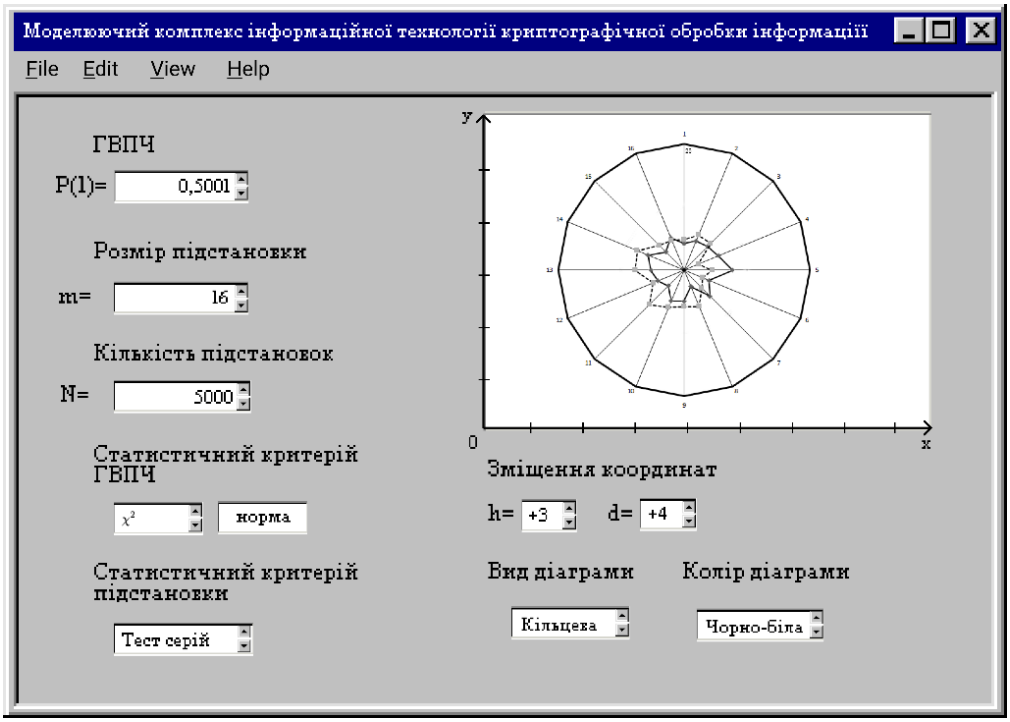


Рис. 8 Скриншот панелі управління моделюючого комплексу інформаційної технології криптографічної обробки інформації в СОІ

Одним із напрям застосування МК ІТ КОІ було проведено перевірку випадковості та рівномірності розподілу потоку підстановок, які утворювалися

за допомогою генератора псевдовипадкових послідовностей на основі сучасних блокових криптоалгоритмів (ДСТУ 7624-2014, AES). Зокрема за формулою 6 було сформовано статистичний аналог матриці перехідних ймовірностей $\mathcal{P}$ перехідних ймовірностей для вузла накладання шифру (табл.8).

Таблиця 8

Статистичний аналог матриці перехідних ймовірностей

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 315 | 308 | 307 | 314 | 317 | 313 | 314 | 316 | 313 | 303 | 307 | 302 | 324 | 314 | 325 | 308 |
| 1 | 313 | 316 | 313 | 314 | 324 | 316 | 311 | 303 | 308 | 312 | 315 | 314 | 314 | 305 | 315 | 307 |
| 2 | 317 | 312 | 303 | 314 | 319 | 291 | 320 | 317 | 327 | 315 | 300 | 319 | 302 | 317 | 315 | 312 |
| 3 | 318 | 307 | 318 | 317 | 310 | 304 | 304 | 326 | 313 | 320 | 306 | 317 | 308 | 311 | 313 | 308 |
| 4 | 315 | 315 | 314 | 310 | 312 | 321 | 309 | 312 | 289 | 304 | 314 | 332 | 307 | 316 | 307 | 323 |
| 5 | 306 | 308 | 326 | 327 | 312 | 326 | 317 | 310 | 312 | 329 | 308 | 299 | 307 | 300 | 305 | 308 |
| 6 | 302 | 306 | 323 | 311 | 309 | 308 | 313 | 300 | 319 | 311 | 325 | 308 | 308 | 313 | 323 | 321 |
| 7 | 305 | 342 | 300 | 317 | 301 | 324 | 314 | 310 | 306 | 317 | 311 | 313 | 309 | 313 | 309 | 309 |
| 8 | 311 | 308 | 318 | 310 | 305 | 306 | 303 | 328 | 326 | 309 | 309 | 330 | 315 | 318 | 302 | 302 |
| 9 | 305 | 317 | 324 | 304 | 319 | 345 | 311 | 316 | 311 | 307 | 315 | 290 | 315 | 313 | 303 | 305 |
| 10 | 308 | 307 | 326 | 307 | 314 | 299 | 307 | 307 | 316 | 316 | 316 | 325 | 317 | 308 | 304 | 323 |
| 11 | 312 | 315 | 314 | 304 | 314 | 310 | 305 | 300 | 332 | 302 | 317 | 312 | 318 | 311 | 310 | 324 |
| 12 | 305 | 318 | 306 | 309 | 309 | 312 | 318 | 337 | 304 | 319 | 313 | 318 | 302 | 315 | 311 | 304 |
| 13 | 337 | 318 | 303 | 305 | 313 | 312 | 313 | 302 | 312 | 304 | 315 | 307 | 315 | 311 | 316 | 317 |
| 14 | 314 | 304 | 295 | 319 | 314 | 308 | 314 | 308 | 304 | 317 | 314 | 311 | 317 | 323 | 311 | 327 |
| 15 | 317 | 299 | 310 | 318 | 308 | 305 | 327 | 308 | 308 | 315 | 315 | 303 | 322 | 312 | 331 | 302 |

Враховуючи складний аналітичний вираз для обчислення цієї матриці за допомогою МК ІТ КОІ, було поставлено експеримент, за допомогою якого з'ясовано що, якщо на вході алгоритму генерації підстановок застосована РРВП, то матриця перехідних ймовірностей наближається до рівноймовірної.

У таблиці 8 наведено значення частот елементів статистичного аналога матриці $\mathcal{P}$ для обсягу вхідних даних $\mathrm{N} = 5 \cdot 10^3$ для $\mathrm{n} = 2^4, \delta = 3$ (для суттєво більшого обсягу даних зменшується наочність подання матриці внаслідок її вельми великого розміру). Графіки перехідних ймовірностей, сформовані на підставі табл.8, наведено на рис.9.

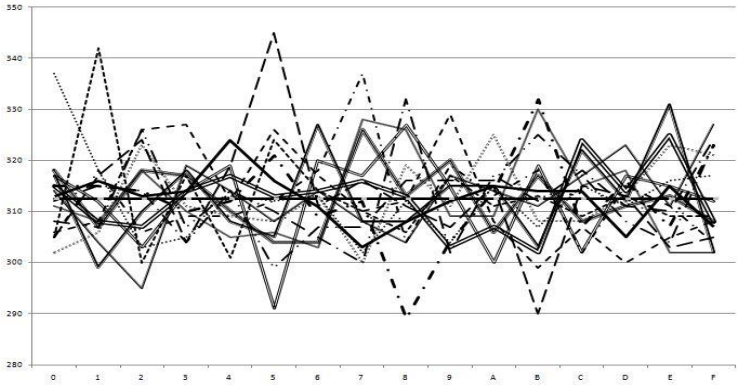


Рис. 9. Графік перехідних ймовірностей

Розподіл зустрічаємості частот у стовпчиках та рядках таблиці 8 в ході експерименту перевірявся за допомогою критерію Пірсона $\chi^2$. Значення статистики Пірсона щодо рівномірного розподілу частот у рядках подано в табл.9.

Таблиця 9

Значення статистики Пірсона згоди для рядків статистичного аналога матриці $\mathcal{P}$

| | Номер рядка | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| $\chi^2$ | 2,04 | 1,2 | 3,99 | 1,94 | 4,15 | 4,49 | 2,81 | 4,73 | 4,03 | 6,69 | 2,96 | 3,15 | 3,58 | 3,32 | 2,91 | 3,88 |

Порівнюючи значення, наведені у табл. 9 з квантілем статистики Пірсона з 15 степенями свободи з рівнем значущості $\alpha = 0{,}05$, $\chi^2_{15,0.05} = 25{,}0$ можливо

зробити висновок, що це добре узгоджується з гіпотезою про рівномірний розподіл частот у статистичному аналогу матриці.

Останнім кроком застосування МК ІТ КОІ було проведено апробацію методу виявлення атак на програмні реалізації засобів КЗІ в СОІ.

Проведення імітаційного моделювання процесу нападу на програмну реалізацію засобу КЗІ (рис. 10) дозволило зробити висновок, що модель підтвердила свою дієздатність. Її застосування в масштабі часу наближеному до реального, дозволило зменшити час на виявлення атаки приблизно на 20%.

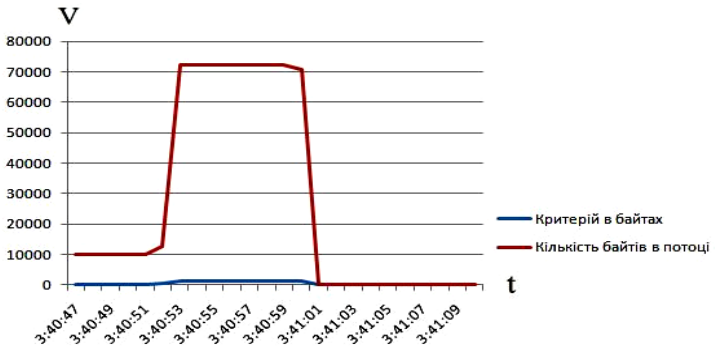


Рис. 10. Графік виявлення атаки

Як висновок, слід констатувати, що в підсумку проведених експериментів було отримано практичні результати, які добре узгоджуються з раніше описаними в розділах методами та моделями.

Останнім кроком дисертаційних досліджень стало удосконалення методу оцінки ефективності застосування криптосистем в СОІ.

Відомо, що у криптографії в якості оцінки ефективності роботи криптосистем, за звичай, використовують співвідношення $^{p}/_{R}$, де $R$ – мінімальна складність методу криптоаналізу, що обчислюється в елементарних операціях обчислювальної техніки, $p$ – ймовірність успішної реалізації цього методу. У роботі ця оцінка набула подальшого розвитку у плані практичного застосування для оцінки відносної ефективності системи захисту інформації в СОІ в умовах кібератак.

Зважаючи на матеріальний характер збитків власника СОІ у разі успіху несанкціонованого втручання у її роботу внаслідок успішної кібератаки та виходячи з необхідності здійснення зловмисником певних матеріальних витрат для реалізації цієї атаки, є логічним у якості оцінки рівня відносної ефективності системи захисту (засобу КЗІ) – величини Q – використовувати дещо інше співвідношення, а саме:

$$Q = \frac{p^{*}\cdot \max(C_{\text{ш}})}{\min\{C_{A1}, C_{A2}, \ldots, C_{Ak}\}},$$

де $C_{\text{ш}}$ – очікувана вартість збитків внаслідок атаки; $C_{A1}, C_{A2}, \ldots, C_{Ak}$ – вартість реалізації відомих атак на систему захисту та їх комбінацій, включаючи крипто аналітичні атаки, атаки на реалізацію та атаки по побічних каналах; $p^{*}$ – ймовірність успішної реалізації кращої атаки.

Логічним кроком постає вибір наступних границь для відносної ефективності системи захисту:

$Q \ll 1$ – високий рівень безпеки, коли очікувана шкода власника СОІ суттєво менше витрат порушника на реалізацію атаки;

$Q \approx 1$ – середній рівень безпеки, коли очікувана шкода власника СОІ практично дорівнює сумі витрат порушника на реалізацію атаки, але сукупність атак може мати більшу ефективність;

$Q \gg 1$ – занадто низький рівень безпеки коли очікувана шкода власника СОІ суттєво перевищує витрати порушника на реалізацію однієї атаки.

Отримані результати дозволили зробити висновок щодо високої конкурентоздатності методів, розроблених в процесі проведення дисертаційних досліджень, що дозволило сформувати рекомендації щодо їх застосування.

## ВИСНОВКИ

У дисертації вирішено актуальне наукове завдання, *яке полягає у розробленні теоретичних і прикладних засад побудови та забезпечення методами криптографічної обробки інформації імітостійкості та конфіденційності даних в СОІ з урахуванням множини кіберзагроз та потенційно можливих наслідків їх реалізації.*

У процесі виконання дисертаційної роботи отримано такі основні результати.

1. Розроблено метод генерації потоку підстановок з використанням шифру БАЗ для забезпечення імітостійкого шифрування в СОІ, впровадження якого дозволяє обрати таку степень підстановок, яка б забезпечувала достатню швидкодію криптоперетворення та була б раціональною для забезпечення захисту повідомлень від підробки.

2. Розроблено метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в СОІ, впровадження якого дозволяє своєчасно виявити момент настання певної критичної ситуації та прийняти рішення щодо подальших дій.

3. Розроблено модель функціонування (криптосхема) шифратора БАЗ (модулю криптографічного захисту інформації) в СОІ, яка є комплексним рішенням в межах двох попередніх методів та впровадження якої дозволяє забезпечити конфіденційність і цілісність інформації, що циркулює в СОІ та в умовах кібератак забезпечити власне функціональну безпеку та живучість самої системи.

4. Удосконалено метод оцінки ефективності застосування криптосистем, який шляхом урахування матеріального характеру збитків власника СОІ у разі успіху несанкціонованого втручання у її роботу, дозволяє визначити границі для відносної ефективності системи захисту інформації в СОІ в умовах реалізації кіберзагроз.

5. Проведено, шляхом імітаційного моделювання процесу нападу на програмну реалізацію засобу КЗІ, експериментальне дослідження моделі функціонування шифратора БАЗ. Це, по-перше, підтвердило дієздатність крипто схеми та, по-друге, в масштабі часу наближеному до реального дозволило впевнитись, що застосування моделі дозволить зменшити час на виявлення атаки приблизно на 20%.

Як результат, в цілому застосування розроблених методів та моделі дозволить:

оперативно приймати рішення щодо подальших дій системи.

знизити ймовірність підробки команди управління до прийнятної для практичного застосування величини, що оцінується величиною $10^{-6}$;

знизити вартість системи виявлення атак на програмні реалізації засобів КЗІ приблизно на 25%;

забезпечити можливість автоматичного переходу ДПЛА в режим автономного виконання завдань в разі виявлення загроз безпеки функціонування системи захисту його радіоканалу управління та передачі даних.

Таким чином, поставлене актуальне наукове завдання розв'язане у повному обсязі. Усі визначені часткові завдання вирішено, мету досліджень досягнуто.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

*Колективна монографія в іноземному науковому виданні:*

1. Opirskyy Ivan. Use of near field communication technology for automated profile replication/ Opirskyy Ivan, Ivanchenko Ihor, Platonenko Artem, **Skladannyi Pavlo**, Roshchuk Mariia. // Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, Bielsko-Biala, Poland. p.153–161.

*Публікації у наукових фахових виданнях України:*

2. Семко В. В. Модель управління захистом інформації в інформаційно-телекомунікаційній системі / В. В. Семко, В. Л. Бурячок, С. В. Толюпа, **П. М. Складанний** // Вісник Національного університету «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації : збірник наукових праць. – 2015. – № 818. – С. 151–155.
3. Семко В.В. Ситуаційне управління доступом в інформаційно-телекомунікаційній системі / В.В.Семко, В.Л. Бурячок, С.В. Толюпа, П**.М. Складанний** // Проблеми телекомунікацій. – 2015. – №2. – С. 54–61.
4. Гулак Г.М. Модель системи виявлення вторгнень з використанням двоступеневого критерію виявлення мережних аномалій / Г.М. Гулак, В.В. Семко, **П.М. Складанний** // Сучасний захист інформації. – 2015. – №4. – С. 81–85.
5. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення / Р.В. Киричок, **П.М. Складанний**, В.Л. Бурячок, Г.М. Гулак, В.А. Козачок // Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №3. – С. 48–61.
6. Гулак Г.М. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах / Г.М. Гулак, В.А. Козачок, **П.М. Складанний** та ін. // Сучасний захист інформації. – 2017. – №2. – С. 65–71.
7. Гулак Г.М. Швидкий алгоритм генерації підстановок багатоалфавітної заміни / Г.М. Гулак, В.Л. Бурячок, **П.М. Складанний** // Захист інформації. – 2017. – №2. – С. 173–177.
8. Гулак Г.М. Забезпечення гарантоздатності автоматизованих систем управління та передачі даних безпілотних літальних апаратів / Г.М. Гулак, **П.М. Складанний**. // Математичні машини та системи. – 2017. - № 3. – С. 154-161.
9. Roy Y.V., Mazur N.P., **Skladannyi P.M**. Audit of Information Security is the basis of Effective Protection of the Enterprise. Cybersecurity: Education, Science, Technique. 2018. No. 1. P. 86—93. URL: https://doi.org/10.28925/2663-4023.2018.1.8693
10. Гулак Г.М., Бурячок В.Л., **Складанний П.М**., Кузьменко Л.В., Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і

заходи протидії шифрувальним вірусам. Кібербезпека: освіта, наука, техніка. Том 2. No10 (2020). – С. 6 – 28.

*Публікації у наукометричних базах Scopus і Web of Science:*

11. Lakhno V., Buriachok V., Parkhuts L., Tarasova H., Kydyralina L., **Skladannyi P**., Skrypnyk M., Shostakovska A. Development of a conceptual model of adaptive access rights management with using the apparatus of Petri nets. International Journal of Civil Engineering & Technology (IJCIET), Volume 9, Issue 11, November 2018. P. 95-104 (**Scopus**).

12. V.Buriachok, V.Sokolov, **P.Skladannyi**. Security Rating Metrics for Distributed Wireless Systems. Proceedings of the 8th International Conference on «Mathematics. Information Technologies. Education» (MoMLeT&DS'2019), June 2–4, 2019: abstracts. —Vol. 2386. —Aachen : CEUR, 2019. — P. . 222–233 :(**Scopus**).

13. Solomentsev O., Zaliskyi M., Skladannyi P. Operation system for modern unmanned aerial vehicles. International Workshop on Cyber Hygiene, CybHyg 2019. 2019. Vol. 2654. P. 363—374. (**Scopus**).

*Тези наукових доповідей:*

14. **Складанний П.М**. Аналіз типів атак на державні інформаційні ресурси. / Складанний П.М. // Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології». – Київ: ДУТ, 2014. – С.20.

15. **Складанний П.М.** Модель загроз безпеки криптосистем. / Складанний П.М. // І Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» (Київ, 20 жовтня 2015р.). – Київ: ДУТ, 2015. – С.35-37.

16. **Складанний П.М.** Псевдовипадкові послідовності та методи захисту інформації. / Складанний П.М. // ІІ Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» (Київ, 12 грудня 2015р.). – Київ: ДУТ, 2015. – С.55.

17. **Складанний П.М.** Визначення критеріїв безпеки криптосистем. / Складанний П.М. // Міжнародна науково-технічна конференція студентства та молоді «Світ телекомунікацій та інформатизації». – Київ: ДУТ, 2015. – С.14-15.

18. **Складанний П.М.** Принцип побудови шифра на основі ГОСТ 28147. / Складанний П.М. // ІІІ Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» (Київ, 02 березня 2016р.). – Київ: ДУТ, 2016 – С.74.

19. Гулак Г.М. Формування вимог щодо забезпечення гарантоздатності автоматизованих систем переробки інформації й управління критично-важливими об'єктами інфраструктури. / Гулак Г.М., **Складанний П.М.** // ІІ Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання» (Одесса, 17 листопада 2017р.). – Одесса: ОДУВС, 2017 – С.12-14.

20. Гулак Г.М. Уточнена модель порушника та модель реалізації кібератак в системах управління технологічними процесами. / Гулак Г.М., Кащук В.І., **Складанний П.М.** // ІХ Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 30 березня 2018р.): Київ: Нац. акад. СБУ, 2018 – С. 47-49

21. Гулак Г.М. Раціональний вибір степені підстановок шифру багатоалфавітної заміни та джерела рівномірно розподіленої випадкової

послідовності. / Гулак Г.М., **Складанний П.М.** // І Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) (Київ, 05-06 квітня 2018 року.) Київ: КНУ імені Т. Шевченка, 2018 – С. 27-31.

## АНОТАЦІЯ

**Складанний П.М. Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації** . – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, Київ, 2021.

Дисертація присвячена розв`язанню актуального наукового завдання, що полягає у розробленні теоретичних і прикладних засад побудови та забезпечення методами криптографічної обробки інформації імітостійкості та конфіденційності даних в СОІ з урахуванням множини кіберзагроз та потенційно можливих наслідків їх реалізації.

У роботі запропоновано моделі та методи, які формують базис для нової моделі функціонування (криптосхеми) шифратора багатоалфавітної заміни (модулю криптографічного захисту інформації) в системах обробки даних.

В масштабі часу наближеному до реального проведено імітаційні експерименти щодо дослідження зазначеної криптосхеми. Отримані результати показали її дієздатність у забезпеченні імітостійкості та конфіденційності інформації, що циркулює в СОІ, а також у забезпеченні в умовах впливу кібератак власне функціональної безпеки та живучості самої системи. Застосування нової моделі шифратора багатоалфавітної заміни дозволило:

визначити границі для відносної ефективності системи захисту інформації в СОІ в умовах кібератак

знизити ймовірність підробки команди управління до прийнятної для практичного застосування величини, що оцінується як $10^{-6}$;

знизити час на виявлення атаки приблизно на 20%

знизити вартість системи виявлення атак на програмні реалізації засобів КЗІ приблизно на 25%;

забезпечити можливість автоматичного переходу ДПЛА в режим автономного виконання завдань в разі виявлення загроз безпеки функціонування системи захисту його радіоканалу управління та передачі даних.

**Ключові слова:** система обробки даних, багатоалфавітна заміна, імітостійкість, криптосхема, криптоалгоритм, криптосистема, криптографічний захист.

# ANNOTATION

**Skladannyi P.M**. **Models and Methods of Ensuring Imitation Resistance and Confidentiality in Information Processing Systems. – Manuscript.**

The dissertation for the degree of a candidate of technical sciences on the specialty 05.13.06 «Information technologies.» Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2021.

The dissertation is devoted to the decision of the actual scientific problem in development of theoretical and applied bases of construction and maintenance by methods of cryptographic processing of the information of imitation stability and confidentiality of the data in SOI taking into account set of cyberthreats and potential consequences of their realization.

The paper proposes models and methods that form the basis for a new model of operation (cryptoscheme) of a multi-alphabetic substitution encoder (module of cryptographic protection of information) in data processing systems.

In the time scale close to the real one, simulation experiments were carried out to study this cryptoschema. The obtained results showed its effectiveness in ensuring the imitation stability and confidentiality of information circulating in the SOI, as well as in providing under the influence of cyberattacks the actual functional security and survivability of the system itself. The use of a new model of multi-alphabetic replacement encoder allowed:

determine the boundaries for the relative effectiveness of the information security system in SOI in cyber attacks

reduce the likelihood of forgery of the management team to an acceptable value for practical use, estimated at $10^{-6}$;

reduce attack detection time by approximately 20%

reduce the cost of the system for detecting attacks on software implementations of CCI by about 25%;

to ensure the possibility of automatic transition of the UAV to the mode of autonomous execution of tasks in case of detection of threats to the security of the protection system of its radio control channel and data transmission.

**Keywords:** data processing system, multi-alphabetic replacement, imitation resistance, cryptoscheme, cryptoalgorithm, cryptosystem, cryptographic protection.