МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

В.о. декана ФКІТ
Ігор ЯКИМЕНКО

_____
«____» _____ 2023 р.

ЗАТВЕРДЖУЮ

В.о. проректора з науково-
педагогічної роботи
Віктор ОСТРОВЕРХОВ

_____
«____» _____ 2023 р.

ЗАТВЕРДЖУЮ
Директор Навчально-наукового
інституту новітніх освітніх технологій
Святослав ПИТЕЛЬ

_____
_____2023 р.

РОБОЧА ПРОГРАМА

з дисципліни «Дослідження і проектування систем захисту інформації»
ступінь вищої освіти – магістр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	1	1	30	15	5	4	96	150	1
Заочна	1	1	8	4	-	-	138	150	1

Тернопіль – 2023

Робоча програма розроблена на основі освітньо-професійної програми підготовки магістра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпеки та захист інформації», затвердженої Вченою радою ЗУНУ (протокол №10 від 23.06.2023 р.).

Робочу програму склав к.т.н., доцент, доцент кафедри кібербезпеки, Якименко Ігор Зіновійович

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол № 1 від 28.08.2023 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол № 1 від 30.08.2023 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “ Дослідження і проектування систем захисту інформації”

Дисципліна – Дослідження і проектування систем захисту інформації	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів – 5	Галузь знань 12 -Інформаційні технології	Статус дисципліни – обов’язкова Мова навчання - українська
Кількість залікових модулів – 4	Спеціальність 125 – Кібербезпека та захист інформації	Рік підготовки: ДФН – 1, ЗФН - 1 Семестр: ДФН – 1, ЗФН – 1
Кількість змістових модулів – 2	Ступінь вишої освіти – магістр	Лекції: ДФН – 30 год., ЗФН - 8 год. Практичні заняття: ДФН – 15 год., ЗФН - 4 год.
Загальна кількість годин – 120		Самостійна робота: ДФН – 100 год, в т. ч. тренінг – 4год., ЗФН – 138 год. Індивідуальна робота: ДФН -5 год.
Тижневих годин: 8 год., з них аудиторних - 3 год.		Вид підсумкового контролю – екзамен

2. Мета й завдання вивчення дисципліни “Дослідження і проектування систем захисту інформації”

2.1. Мета завдання дисципліни

Мета вивчення дисципліни “Дослідження і проектування систем захисту інформації” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу “Дослідження і проектування систем захисту інформації» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Кібернетична безпека», «Криптографія», «Дискретна математика»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни.

В результаті вивчення курсу „ Дослідження і проектування систем захисту інформації ” студенти повинні:

- засвоїти основні фундаментальні поняття і закони захисту інформації для їх використання в сучасних системах;
- знати принципи побудови криптографічних алгоритмів, криптографічних стандартів та їх використання в задачах захисту інформації;
- використовувати основні математичний апарат та закони криптографії в професійній діяльності;
- вміти використовувати програмні засоби, які реалізують основні криптографічні функції;
- здатні до програмної реалізації алгоритмів вирішення типових задач захисту інформації;
- здатні проектувати різного рівня системи захисту;
- вміти використовувати методи та засоби криптографічного захисту даних.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

- здатність до абстрактного мислення, аналізу та синтезу;
- здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки;
- здатність розробляти, впроваджувати та аналізувати нормативні документи,

положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки;

– здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури;

– здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

– застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, науково-технічні методи і моделі, фізичні та математичні фундаментальні знання в галузі інформаційної безпеки та/або кібербезпеки;

– досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури;

– провадити дослідження, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також проводити аналіз і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури;

– обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації;

– мати навички керування, розроблення, впровадження та супроводження проектів з забезпечення інформаційної безпеки та/або кібербезпеки.

2.4. Передумови для вивчення дисципліни

Вивчення курсу „Дослідження і проектування систем захисту інформації” передбачає наявність систематичних та ґрунтовних знань із суміжних курсів «Основи кібербезпеки», «Безпека комп’ютерних мереж», «Крипторграфія» та ін.., а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.5 Результати навчання.

Знання теоретичних основ захисту інформації, засобів проектування систем захисту інформації, сучасних систем захисту інформації.

3. Програма навчальної дисципліни “Дослідження і проектування систем захисту інформації"

Змістовий модуль 1. Загальні положення щодо захисту інформації в комп'ютерних системах

Тема 1. Теоретичні засади дослідження та проектування систем захисту інформації. Принципи організації захисту інформації. Концепція національної безпеки України, концепція інформаційної безпеки України, доктрина інформаційної безпеки України. Основні поняття, терміни та визначення.

Література: 1-18.

Тема 2. Технічний захист інформації. Технічний захист відомостей з обмеженим доступом. Технічна охорона об’єктів. Організація та контроль технічного захисту в Україні . Місце технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації. Основні поняття, терміни та визначення технічного захисту інформації. Види інформації, яка може стати об’єктом злочинних посягань. Поняття технічних каналів витоку інформації та механізм їх утворення. Визначення можливих джерел витоку інформації з радіоканалу.

Література: 1-18.

Тема 3. Міжнародні стандарти у галузі інформаційної безпеки. Стандарти і специфікації в галузі безпеки інформаційних систем. «Помаранчева книга» як оцінний стандарт. Класи безпеки інформаційних систем. Технічна специфікація X.800 Стандарт ISO/IEC 15408. Розвиток стандартів з управління ризиками. Стандарт ISO/IEC TR 13335

Література: 1-18.

Змістовий модуль 2. Теоретико-числові базиси та системи числення

Тема 4. Теоретичні основи цілочисельної системи залишкових класів (СЗК).

Література: 1-18.

Тема 5. Симетричний метод шифрування у СЗК та на основі Китайської теореми про залишки.

Література: 1-18.

Тема 6. Асиметричний метод шифрування у СЗК.

Література: 1-18.

Тема 7. Нормалізована форма СЗК. Досконалі форми СЗК.

Література: 1-18.

Тема 8. Міжбазисні перетворення на основі розмежованої СЗК.

Література: 1-18.

Тема 9. Ступінчата СЗК. Метод шифрування у ступінчатій СЗК.

Література: 1-18.

Тема 10. Дослідження стійкості симетричних алгоритмів шифрування у СЗК та на основі Китайської теореми про залишки.

Література: 1-18.

Тема 11. Дослідження стійкості асиметричних методів шифрування у СЗК.

Література: 1-18.

Тема 12. Метод пошуку оберненого поліному за модулем на основі методу невизначених коефіцієнтів.

Література: 1-18.

Тема 13. Метод відновлення поліномів за його залишками.

Література: 1-18.

Тема 14. Метод шифрування у поліноміальній системі залишкових класів.

Література: 1-18.

Тема 15. Дослідження стійкості методу шифрування у поліноміальній системі залишкових класів.

Література: 1-18.

4. Структура залікового кредиту дисципліни “ Дослідження і проектування систем захисту інформації ”

ДФН

	Кількість годин					
	Лекції	Практ. заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Загальні положення цифрової криміналістики						
Тема 1. Теоретичні засади дослідження та проектування систем захисту інформації.	2	1	6		1	Поточне опитування
Тема 2. Технічний захист інформації.	2	1	6	0,25		Поточне опитування
Тема 3. Міжнародні стандарти у галузі інформаційної безпеки.	2	1	6	0,25		Поточне опитування
Змістовий модуль 2. Методи шифрування у системі залишкових класів						
Тема 4. Теоретичні основи цілочисельної СЗК базису Крестенсона.	2	1	5	0,25	3	Поточне опитування
Тема 5. Симетричний метод шифрування у СЗК та на основі Китайської теореми про залишки.	2	1	5	0,25		Поточне опитування
Тема 6. Асиметричний метод шифрування у СЗК.	2	1	5	0,25		Поточне опитування

Тема 7. Нормалізована форма СЗК. Досконалі форми СЗК.	2	1	5	0,25		Поточне опитування
Тема 8. Міжбазисні перетворення на основі розмежованої СЗК.	2	1	5	0,25		Поточне опитування
Тема 9. Ступінчата СЗК. Метод шифрування у ступінчатій СЗК..	2	1	5	0,25		Поточне опитування
Тема 10. Дослідження стійкості симетричних алгоритмів шифрування у СЗК та на основі Китайської теореми про залишки	2	1	8	0,5		Поточне опитування
Тема 11. Дослідження стійкості асиметричних методів шифрування у СЗК..	2	1	8	0,5		Поточне опитування
Тема 12. Метод пошуку оберненого поліному за модулем на основі методу невизначених коефіцієнтів.	2	1	8	0,5		Поточне опитування
Тема 13. Метод відновлення поліномів за його залишками.	2	1	8	0,5		Поточне опитування
Тема 14. Метод шифрування у поліноміальній системі залишкових класів.	2	1	8	0,5		Поточне опитування
Тема 15. Дослідження стійкості методу шифрування у поліноміальній системі залишкових класів	2	1	8	0,5		Поточне опитування
Разом	**30**	**15**	**100**	**5**	**4**	**Іспит**

ЗФН

	Кількість годин			
	Лекції	Практ. заняття	СРС	Контрольні заходи
Змістовий модуль 1. Загальні положення цифрової криміналістики				
Тема 1. Теоретичні засади дослідження та проектування систем захисту інформації.	0,5	1	6	Поточне опитування
Тема 2. Технічний захист інформації.	0,5		6	Поточне опитування
Тема 3. Міжнародні стандарти у галузі інформаційної безпеки.	0,5		6	Поточне опитування
Змістовий модуль 2. Теоретико-числові базиси та системи числення				
Тема 4. Теоретичні основи цілочисельної СЗК базису Крестенсона.	0,5	1	8	Поточне опитування
Тема 5. Симетричний метод шифрування у СЗК та на основі Китайської теореми про залишки.	0,5		8	Поточне опитування
Тема 6. Асиметричний метод шифрування у СЗК.	0,5		10	Поточне опитування
Тема 7. Нормалізована форма СЗК. Досконалі форми СЗК.	0,5		10	Поточне опитування
Тема 8. Міжбазисні перетворення на основі розмежованої СЗК.	0,5		10	Поточне опитування
Тема 9. Ступінчата СЗК. Метод шифрування у ступінчатій СЗК..	0,5	1	10	Поточне опитування
Тема 10. Дослідження стійкості симетричних алгоритмів шифрування у СЗК та на основі Китайської теореми про залишки	0,5		10	Поточне опитування
Тема 11. Дослідження стійкості асиметричних методів шифрування у СЗК..	0,5		10	Поточне опитування

Тема 12. Метод пошуку оберненого поліному за модулем на основі методу невизначених коефіцієнтів.	0,5	1	10	Поточне опитування
Тема 13. Метод відновлення поліномів за його залишками.	0,5		10	Поточне опитування
Тема 14. Метод шифрування у поліноміальній системі залишкових класів.	1		10	Поточне опитування
Тема 15. Дослідження стійкості методу шифрування у поліноміальній системі залишкових класів	0,5		10	Поточне опитування
Разом	**8**	**4**	**138**	**Іспит**

5. Тематика практичних занять.

Практичне заняття №1

Тема: Теоретичні основи цілочисельної СЗК базису Крестенсона.
Мета: Застосування теоретичних основ цілочисельної СЗК базису Крестенсона.
Питання для обговорення: Теоретичні основи цілочисельної СЗК базису Крестенсона.
Література: 1-18.

Практичне заняття № 2

Тема: Симетричний метод шифрування у СЗК.
Мета: Приклади симетричного методу шифрування у СЗК.
Питання для обговорення: Симетричний метод шифрування у СЗК.
Література: 1-18.

Практичне заняття №3

Тема: Асиметричний метод шифрування у СЗК.
Мета: Приклади асиметричного методу шифрування у СЗК.
Питання для обговорення: Асиметричний метод шифрування у СЗК.
Література: 1-18.

Практичне заняття №4

Тема: Нормалізована форма СЗК. Досконалі форми СЗК.
Мета: Критерії досконалих форм СЗК.
Питання для обговорення: Досконалі форми СЗК.
Література: 1-18.

Практичне заняття №5

Тема: Міжбазисні перетворення на основі розмежованої СЗК.
Мета: Задачі пов’язані з міжбазисними перетвореннями на основі розмежованої СЗК.
Питання для обговорення: Базиси, міжбазисні перетворення на основі розмежованої СЗК.
Література: 1-18.

Практичне заняття № 6

Тема: Ступінчата СЗК.
Мета: Фундаментальні прикладні задачі у ступінчатій СЗК..
Питання для обговорення: Ступінчата СЗК
Література: 1-18.

Практичне заняття № 7

Тема: Метод шифрування у ступінчатій СЗК.
Мета: Приклади методу шифрування у ступінчатій СЗК.
Питання для обговорення: Теоретичні основи методу шифрування у ступінчатій СЗК.
Література: 1-18.

Практичне заняття № 8

Тема: Симетричний метод шифрування на основі Китайської теореми про залишки.
Мета: Застосування теоретичних основ симетричного методу шифрування на основі Китайської теореми про залишки.
Питання для обговорення: Симетричний метод шифрування на основі Китайської теореми про залишки.
Література**:** 1-18

Практичне заняття № 9

Тема: Теорія чисел.

Мета: Вирішення прикладних задач теорії чисел на основі модульних операцій базису Крестенсона.

Питання для обговорення: основні визначення та поняття.

Література: 1-18.

Практичне заняття № 10

Тема: Дослідження стійкості симетричних алгоритмів шифрування у СЗК та на основі Китайської теореми про залишки.

Мета: Дослідження стійкості симетричних алгоритмів шифрування у СЗК на основі асимтотичного розподілу простих чисел.

Питання для обговорення: Стійкість симетричних алгоритмів шифрування у СЗК та на основі Китайської теореми про залишки.

Література: 1-18.

Практичне заняття № 11

Тема: Дослідження стійкості симетричних алгоритмів шифрування у СЗК та на основі Китайської теореми про залишки.

Мета: Дослідження стійкості симетричних алгоритмів шифрування у СЗК на основі функції Ейлера.

Питання для обговорення: Методи дослідження стійкості.

Література: 1-18.

Практичне заняття № 12

Тема: Метод пошуку оберненого поліному за модулем на основі методу невизначених коефіцієнтів.

Мета: Використання теорії пошуку оберненого поліному за модулем на основі методу невизначених коефіцієнтів.

Питання для обговорення: основні визначення та поняття.

Література: 1-18.

Практичне заняття № 13

Тема: Метод відновлення поліномів за його залишками.

Мета: Використання теорії відновлення поліномів за його залишками.

Питання для обговорення: Метод відновлення поліномів за його залишками на основі КТЗ.

Література: 1-18.

Практичне заняття № 14

Тема: Метод шифрування у поліноміальній системі залишкових класів.

Мета: Використання теорії шифрування у поліноміальній системі залишкових класів.

Питання для обговорення: основні теоретичні положення методу шифрування у поліноміальній системі залишкових класів.

Література: 1-18.

Практичне заняття № 15

Тема: Дослідження стійкості методу шифрування у поліноміальній системі залишкових класів.

Мета: Використання теорії дослідження стійкості методу шифрування у поліноміальній системі залишкових класів на основі функції Мебіуса.

Питання для обговорення: методи дослідження стійкості.

Література: 1-18.

6. Комплексне практичне індивідуальне завдання (КПІЗ).

Індивідуальне завдання з курсу "Дослідження і проектування систем захисту інформації" виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Метою виконання КПІЗ є оволодіння навиками дослідження та проектування систем захисту інформації.

Варіанти КПІЗ:

Теоретичні основи цілочисельної СЗК базису Крестенсона.

Кодування інформаційних потоків в СЗК з довільним порядком реєстрації даних.
Каскадне кодування даних на основі методу залишків та СЗК.
Нормалізована форма СЗК. Досконалі форми СЗК.
Критерії досконалих форм СЗК.
Міжбазисні перетворення на основі розмежованої СЗК.
Задачі пов'язані з міжбазисними перетвореннями на основі розмежованої СЗК.
Теоретико-числовий базис Крестенсона.
Використання теоретико-числового базису базису Крестенсона.
Знаходження найбільшого спільного дільника з використання базису Крестенсона.
Алгоритм Евкліда в розмежованій системі числення.
Фундаментальні прикладні задачі у базисі Крестенсона.
Теорія чисел.
Вирішення прикладних задач теорії чисел на основі модульних операцій базису Крестенсона.
Алгоритм піднесення до високих показників степенів у розмежованій системі числення базису Крестенсона-Радемахера в задачах захисту інформації.
Використання алгоритму піднесення до високих показників степенів у розмежованій системі числення базису Крестенсона-Радемахера в задачах захисту інформації.

Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту.

7. Самостійна робота

№ п/п	Тематика
1	Математичні основи теоретико-числових базисів.
2	Теоретико-числові базиси на основі кусково-постійних ортогональних функцій.
3	Унітарний базис та базис Хаара.
4	Базис Радемахера та Лібова-Крейга.
5	Базис Уолша та ортогональних функцій Грея.
6	Базис Крестенсона.
7	Базис та кодові системи Галуа
8	Тренінг
Разом	

8. Тренінг з дисципліни

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Тематика тренінгу: Застосування теорії множин та графів при дослідженні оптимізаційних задач проектування систем захисту інформації.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни "Дослідження і проектування систем захисту інформації" використовуються наступні методи оцінювання навчальної роботи студента:

- поточне опитування;
- залікове модульне тестування та опитування;
- презентації результатів виконаних завдань;
- оцінювання результатів КПІЗ;
- завдання на лабораторному обладнанні, тощо;
- ректорська контрольна робота;
- екзамен;
- інші види індивідуальних та групових завдань.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни “Дослідження і проектування систем захисту інформації” визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «**Дослідження та проектування систем захисту інформації**» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для екзамену

	Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4 (екзамен)
	20%	20%	20%	40%
	1. Усне опитування на заняттях – max 20 балів. 2. Письмова робота – max 50 балів. 3. Практичне завдання – max 30 балів	1. Усне опитування на заняттях – max 20 балів. 2. Письмова робота – max 50 балів. 3. Практичне завдання – max 30 балів	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг – max 30 балів	1. Розв’язання 20 тестів по 3 бали = max 60 балів. 2. Практичне завдання = max 40 балів

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Електронний варіант лекцій	1 -15
2	Методичні вказівки до виконання практичних робіт (електронний варіант)	1 - 12
3	Обладнання: Проектор, комп’ютери з доступом до мережі Інтернету. Програмне забезпечення: FoxitReader, WinZip, Total Commander, Dev C++, Python 3.5.8, Visual Studio community edition	1- 12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.

2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, NIST Special Publication 800-12 Revision 1 An Introduction to Information Security Michael Nieles Kelley Dempsey Victoria Yan Pillitteri

3. Milov O., Kazakova N., Milczarski P., Korol O. Mechanisms of cyber security: the problem of conceptualization // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 2, pp. 110-116.

4. Information Security in an Organization Mohammed Mahfouz Alhassan, Alexander Adjei-Quaye International Journal of Computer (IJC) (2017) Volume 24, No 1, pp 100-116.

5. Спеціалізовані комп'ютерні технології в інформатиці. / під редакцією Николайчука Я.М.– Тернопіль: ТзОВ "Терно-граф".,2017 – С. 912.

6. Yakymenko I., Ivas'ev S., Kasianchuk M. High-Productivity Methods Of Finding Residues Multidigital Numbers By Modulo/ Колективна монографія/"Engineer of XXI Century" – the VI Inter University Conference of Students, PhD Students and Young Scientists, University of Bielsko-Biała (ATH) – Bielsko-Biała, Poland, 2016. – 922 p.

7. Etienne Lemaire. Pretty Modular Symmetric Encryption (PMSE), compact algorithm for "embedded cryptography" with quite low computational cost. 2019. ffhal-02131858

8. V. Migliore, M. M. Real, V. Lapotre, A. Tisserand, C. Fontaine and G. Gogniat, "Fast polynomial arithmetic for Somewhat Homomorphic Encryption operations in hardware with Karatsuba algorithm," *2016 International Conference on Field-Programmable Technology (FPT)*, Xi'an, China, 2016, pp. 209-212, doi: 10.1109/FPT.2016.7929535.

9. C. Jayet-Griffon, M. . -A. Cornelie, P. Maistri, P. Elbaz-Vincent and R. Leveugle, "Polynomial multipliers for fully homomorphic encryption on FPGA," *2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Riviera Maya, Mexico, 2015, pp. 1-6, doi: 10.1109/ReConFig.2015.7393335.

10. Jianhua Wu, Hai Liu, Xishun Zhu Image encryption based on permutation polynomials over finite fields Optica Applicata, Vol. L, No. 3, 2020, pp. 357-376. DOI: 10.37190/oa200303

11. Alamsyah, A. Bejo, and T. B. Adji, "The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box". *Nonlinear Dynamics*, vol. 93, no. 4, pp. 2105–2118, 2018.

12. Alamsyah, A. A Novel Construction of Perfect Strict Avalanche Criterion S-box using Simple Irreducible Polynomials May 2020 Scientific Journal of Informatics 7(1):10-22 DOI:10.15294/sji.v7i1.24006

13. P. Agarwal, A. Singh and A. Kilicman, "Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant", Advances in Mechanical Engineering, vol. 10, no. 7, pp. 1-18, 2018.

14. Kouther Fahad Alshammaria,* , Ayman Mostafaa , Shadi Nashwana Avalanche Analysis of Variant Polynomials for AES Turkish Journal of Computer and Mathematics Education Vol.12 No.14(2021), 2696- 2703

15. D. Schinianakis and T. Stouraitis, "Multifunction Residue Architectures for Cryptography," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 4, pp. 1156-1169, April 2014, doi: 10.1109/TCSI.2013.2283674.

16. Tynymbayev, Sakhybay and Ibraimov, Margulan and Namazbayev, Timur and Gnatyuk, Sergiy, Development of Pipelined Polynomial Multiplier Modulo Irreducible Polynomials For Cryptosystems (February 25, 2022). Eastern-European Journal of Enterprise Technologies, 1 (4 (115)), 37–43, 2022, doi: https://doi.org/10.15587/1729-4061.2022.251913

17. Laurent-Stéphane Didier, Fangan-Yssouf Dosso, Nadia El Mrabet, Jérémy Marrez, Pascal Véron. Randomization of Arithmetic over Polynomial Modular Number System. 26th IEEE International Symposium on Computer Arithmetic, Jun 2019, Kyoto, Japan. pp.199-206, ff10.1109/ARITH.2019.00048ff. ffhal-02099713f

18. Idris Abiodun Aremu, Kazeem Alagbe Gbolagade. Redundant Residue Number System Based Multiple Error Detection and Correction Using Chinese Remainder Theorem (CRT). Software Engineering. Vol. 5, No. 5, 2017, pp. 72-80. doi: 10.11648/j.se.20170505.12