**Государственное образовательное учреждение**
**«Приднестровский государственный университет им. Т.Г. Шевченко»**

**Инженерно-технический институт**

**Кафедра «Информационные технологии и автоматизированное управление производственными процессами»**

УТВЕРЖДАЮ
Директор института, доцент
_____ Ф.Ю. Бурменко
«30» сентября 2022 г.

# РАБОЧАЯ ПРОГРАММА

**по дисциплине**

**Б1.О.09 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

на 2022/2023 учебный год

Направление

**2.09.04.02 Информационные системы и технологии**

Профиль
**Защита информации в информационных системах**

Квалификация

**магистр**

Форма обучения
**очная, заочная**

2022 ГОД НАБОРА

Тирасполь 2022 г.

Рабочая программа дисциплины **Криптографические методы защиты информации** разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки **2.09.04.02 Информационные системы и технологии** и основной профессиональной образовательной программы (учебного плана) по профилю подготовки **Защита информации в информационных системах**.

Составители рабочего программы

Доцент, к.т.н. Т.Д.Бордя

Рабочая программа утверждена на заседании кафедры *информационных технологий и автоматизированного управления производственными процессами*

29 августа 2022 г. протокол № 1

Зав. кафедрой ИТиАУПП

29 августа 2022 г. Ю.А.Столяренко

## 1. Цели и задачи освоения дисциплины (модуля)

**Цели** освоения дисциплины «Криптографические методы защиты информации» являются познакомить магистрантов с вопросами применения криптографических протоколов для защиты информации в современных информационно - телекоммуникационных системах.

Задачами освоения дисциплины «Криптографические методы защиты информации» являются, что слушатели по окончании изучения дисциплины должны знать, уметь и применять основные принципы организации криптографической защиты информации.

## 2. Место дисциплины в структуре ОПОП

Шифр дисциплины в учебном плане Б1.О.09

Дисциплина относится к обязательной части блока Б1 учебного плана направления 2.09.04.02 Информационные системы и технологии в соответствии с Государственным образовательным стандартом ВО.

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

## 3.Требования к результатам освоения дисциплины (модуля):

*Изучение дисциплины направлено на формирование компетенций, приведенных в таблице ниже*

| **Категория общепрофессиональных компетенций** | **Код и наименование общепрофессиональной компетенции** | **Код и наименование индикатора достижения общепрофессиональной компетенции** |
|---|---|---|
| ***Общепрофессиональные компетенции выпускников и индикаторы их достижения*** | | |
| - | ОПК-1. Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте | ИД-1$_{ОПК-1}$ Знать математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности |
| | | ИД-2$_{ОПК-1}$ Уметь решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных социально-экономических и профессиональных знаний |
| | | ИД-3$_{ОПК-1}$ Иметь навыки: теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте |

## 4.Структура и содержание дисциплины (модуля)

***4.1. Распределение трудоемкости в з.е./часах по видам аудиторной и самостоятельной работы студентов по семестрам:***

| Форма обучения | Семестр (оч.ф), Курс (з.ф) | Трудоемкость,з.е./часы | Количество часов | | | | | Форма контроля |
|---|---|---|---|---|---|---|---|---|
| | | | В том числе | | | | Самостоятельная работа (СР) | |
| | | | Аудиторных | | | | | |
| | | | Всего | Лекций (Л) | Практических (ПЗ) | Лабораторных занятий (ЛЗ) | | |
| Очная | 2 | 3/108 | 42 | 28 | | 14 | 66 | Зачет |
| | **Итого:** | 3/108 | 42 | 28 | | 14 | 66 | Зачет |
| Заочная | 1 (Летняя сессия) | 3/108 | 16 | 8 | | 8 | 88 | Зачет (4ч) |
| | **Итого:** | 3/108 | 16 | 8 | | 8 | 88 | Зачет (4ч) |

***4.2. Распределение видов учебной работы и их трудоемкости по разделам дисциплины***

| № Раздела | Наименование раздела | Количество часов | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Всего | | Аудиторная работа | | | | | | СР | |
| | | | | Л | | ПЗ | | ЛЗ | | | |
| | | оч.ф | з.ф | оч.ф | з.ф | оч.ф | з.ф | оч.ф | з.ф | оч.ф | з.ф |
| 1 | Криптосистемы с открытым ключом. | 10 | 10 | 4 | 2 | - | - | 2 | 2 | 4 | 6 |
| 2 | Методы взлома шифров, основанных на дискретном логарифмировании. | 10 | 10 | 4 | 2 | - | - | 2 | 2 | 4 | 6 |
| 3 | Цифровая подпись. | 18 | 18 | 4 | 2 | - | - | 4 | 2 | 10 | 14 |
| 4 | Криптографические протоколы. | 18 | 18 | 4 | 2 | - | - | 4 | 2 | 10 | 14 |
| 5 | Криптосистемы на эллиптических кривых. | 16 | 16 | 4 | - | - | - | - | - | 12 | 16 |
| 6 | Теоретическая стойкость криптосистем. | 18 | 16 | 4 | - | - | - | 2 | - | 12 | 16 |
| 7 | Современные шифры с секретным ключом. | 18 | 16 | 4 | - | - | - | - | - | 14 | 16 |
| **Всего** | | 108 | 104 | 28 | 8 | - | - | 14 | 8 | 66 | 88 |
| **Контроль** | | | 4 | | | | | | | | 4 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Итого** | 108 | 108 | 28 | 8 | - | - | 14 | 8 | 66 | 92 |

### *4.3. Тематический план по видам учебной деятельности*

***Лекции***

| № п/п | Номер раздела дисциплины | Объем часов | | Тема лекций | Учебно-наглядные пособия |
|---|---|---|---|---|---|
| | | **ПО** | **ФЗ** | | |
| Криптосистемы с открытым ключом | | | | | |
| 1 | 1 | 2 | 2 | Арифметика остатков | Презентация |
| 2 | 1 | 2 | | Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. | Презентация |
| Итого по разделу часов: | | **4** | **2** | | |
| Методы взлома шифров, основанных на дискретном логарифмировании | | | | | |
| 3 | 2 | 2 | 2 | Метод «Шаг младенца, шаг великана». | Презентация |
| 4 | 2 | 2 | | Алгоритм исчисления порядка. | Презентация |
| Итого по разделу часов: | | **4** | **2** | | |
| Цифровая подпись. | | | | | |
| 5 | 3 | 2 | 2 | Электронная подпись RSA. | Презентация |
| 6 | 3 | 2 | | Электронная подпись на базе шифра Эль-Гамаля. Стандарты на цифровую подпись. | Презентация |
| Итого по разделу часов: | | **4** | **2** | | |
| Криптографические протоколы | | | | | |
| 7 | | 2 | 2 | Электронные деньги. | Презентация |
| 8 | | 2 | | Взаимная идентификация с установлением ключа. | Презентация |
| Итого по разделу часов: | | **4** | **2** | | |
| Криптосистемы на эллиптических кривых. | | | | | |
| 9 | | 2 | - | Математические основы. Выбор параметров кривых. | Презентация |
| 10 | | 2 | | Построение криптосистем на эллиптических кривых. | Презентация |
| Итого по разделу часов: | | **4** | **-** | | |
| Теоретическая стойкость криптосистем | | | | | |
| 11 | | 2 | | Теория систем с совершенной секретностью. Шифр Вернама. | Презентация |
| 12 | | 2 | | Элементы теории информации. Расстояние единственности шифра с секретным ключом. Идеальные криптосистемы. | Презентация |
| Итого по разделу часов: | | **4** | **-** | | |
| Современные шифры с секретным ключом | | | | | |

| | | | | |
|---|---|---|---|---|
| 13 | 2 | - | Элементы теории информации. Расстояние единственности шифра с секретным ключом. Идеальные криптосистемы. | Презентация |
| 14 | 3 | | Современные блоковые и поточные шифры. Криптографические хеш-функции. | Презентация |
| Итого по разделу часов: | **4** | - | | |
| **ИТОГО:** | **28** | **8** | | |

***Практические (семинарские) занятия***

Учебным планом не предусмотрены.

***Лабораторные занятия***

| № п/п | Номер раздела дисциплины | Объем часов | | Тема лекций | Учебно-наглядные пособия |
|---|---|---|---|---|---|
| | | оч. ф. | з. ф. | | |
| Криптосистемы с открытым ключом | | | | | |
| 1 | 1 | 2 | 2 | Криптосистемы с открытым ключом. | МР; КЗ |
| Итого по разделу часов: | | **2** | **2** | | |
| Методы взлома шифров, основанных на дискретном логарифмировании | | | | | |
| 2 | 2 | 2 | 2 | Метод «Шаг младенца, шаг великана». Алгоритм исчисления порядка. | МР; КЗ |
| Итого по разделу часов: | | **2** | **2** | | |
| Цифровая подпись. | | | | | |
| 3 | 3 | 2 | 2 | Электронная подпись RSA, Эль-Гамаля | МР; КЗ |
| 4 | 3 | 2 | | Стандарты на цифровую подпись. | МР; КЗ |
| Итого по разделу часов: | | **4** | **2** | | |
| Криптографические протоколы | | | | | |
| 5 | 4 | 2 | 2 | Доказательство с нулевым знанием | МР; КЗ |
| 6 | 4 | 2 | | Криптографические протоколы. | МР; КЗ |
| Итого по разделу часов: | | **4** | **2** | | |
| Теоретическая стойкость криптосистем. | | | | | |
| 7 | 6 | 2 | - | Теоретическая стойкость криптосистем. | МР; КЗ |
| Итого по разделу часов: | | **2** | **-** | | |
| **ИТОГО:** | | **14** | **8** | | |

***Самостоятельная работа обучающегося по очной форме обучения***

| Раздел дисциплины | № п/п | Тема и вид самостоятельной работы обучающегося | Трудоемкость (в часах) |
|---|---|---|---|
| Криптосистемы с открытым ключом | | | |
| Раздел 1 | 1 | Арифметика остатков. Функция Эйлера. Алгоритм Евклида. Быстрые алгоритмы возведения в степень. | 2 |
| | 2 | Односторонние функции. Система Диффи-Хеллмана. | 2 |
| | | **Итого по разделу часов** | **4** |
| Методы взлома шифров, основанных на дискретном логарифмировании | | | |
| Раздел 2 | 1 | Методы взлома шифров, основанных на дискретном логарифмировании. Шаг «младенца», шаг «великана» | 2 |
| | 2 | Методы взлома шифров, основанных на дискретном логарифмировании. Исчисление порядка | 2 |
| | | **Итого по разделу часов** | **4** |
| Цифровая подпись. | | | |
| Раздел 3 | 1 | Электронная подпись RSA. | 2 |
| | 2 | Электронная подпись на базе шифра Эль-Гамаля. | 4 |
| | 3 | Стандарты на цифровую подпись. | 4 |
| | | **Итого по разделу часов** | **10** |
| Криптографические протоколы | | | |
| Раздел 4 | 1 | Ментальный покер. | 2 |
| | 2 | Доказательства с нулевым знанием. | 2 |
| | 3 | Электронные деньги. | 2 |
| | 4 | Взаимная идентификация с установлением ключа. | 4 |
| | | **Итого по разделу часов** | **10** |
| Криптосистемы на эллиптических кривых. Теоретическая стойкость криптосистем | | | |
| Раздел 5 | 1 | Математические основы. Выбор параметров кривых. | 6 |
| | 2 | Построение криптосистем на эллиптических кривых. | 6 |
| | | **Итого по разделу часов** | **12** |
| Теоретическая стойкость криптосистем | | | |
| Раздел 6 | 1 | Теория систем с совершенной секретностью. Шифр Вернама. | 6 |
| | 2 | Элементы теории информации. Расстояние единственности шифра с секретным ключом. Идеальные криптосистемы. | 6 |
| | | **Итого по разделу часов** | **12** |
| Современные шифры с секретным ключом Случайные числа в криптографии. | | | |
| Раздел 7 | 1 | Теория систем с совершенной секретностью. Шифр Вернама. | 4 |
| | 2 | Элементы теории информации. Расстояние единственности шифра с секретным ключом. Идеальные криптосистемы. | 4 |

| Раздел дисциплины | № п/п | Тема и вид самостоятельной работы обучающегося | Трудоемкость (в часах) |
|---|---|---|---|
| | 3 | Современные блоковые и поточные шифры. Криптографические хеш-функции. | 6 |
| | | **Итого по разделу часов** | **14** |
| | | **ИТОГО:** | **66** |

***Самостоятельная работа обучающегося по заочной форме обучения***

| Раздел дисциплины | № п/п | Тема и вид самостоятельной работы обучающегося | Трудоемкость (в часах) |
|---|---|---|---|
| Криптосистемы с открытым ключом | | | |
| Раздел 1 | 1 | Арифметика остатков. Функция Эйлера. Алгоритм Евклида. Быстрые алгоритмы возведения в степень. | 2 |
| | 2 | Односторонние функции. Система Диффи-Хеллмана. | 4 |
| | | **Итого по разделу часов** | **6** |
| Методы взлома шифров, основанных на дискретном логарифмировании | | | |
| Раздел 2 | 1 | Методы взлома шифров, основанных на дискретном логарифмировании. Шаг «младенца», шаг «великана» | 2 |
| | 2 | Методы взлома шифров, основанных на дискретном логарифмировании. Исчисление порядка | 4 |
| | | **Итого по разделу часов** | **6** |
| Цифровая подпись. | | | |
| Раздел 3 | 1 | Электронная подпись RSA. | 4 |
| | 2 | Электронная подпись на базе шифра Эль-Гамаля. | 4 |
| | 3 | Стандарты на цифровую подпись. | 6 |
| | | **Итого по разделу часов** | **14** |
| Криптографические протоколы | | | |
| Раздел 4 | 1 | Ментальный покер. | 2 |
| | 2 | Доказательства с нулевым знанием. | 4 |
| | 3 | Электронные деньги. | 4 |
| | 4 | Взаимная идентификация с установлением ключа. | 4 |
| | | **Итого по разделу часов** | **14** |
| Криптосистемы на эллиптических кривых. | | | |
| Раздел 5 | 1 | Математические основы. Выбор параметров кривых. | 6 |
| | 2 | Построение криптосистем на эллиптических кривых. | 10 |
| | | **Итого по разделу часов** | **16** |
| Теоретическая стойкость криптосистем | | | |
| Раздел 6 | 1 | Теория систем с совершенной секретностью. Шифр Вернама. | 6 |

| Раздел дисциплины | № п/п | Тема и вид самостоятельной работы обучающегося | Трудоемкость (в часах) |
|---|---|---|---|
| | 2 | Элементы теории информации. Расстояние единственности шифра с секретным ключом. Идеальные криптосистемы. | 10 |
| | | **Итого по разделу часов** | **16** |
| Современные шифры с секретным ключом | | | |
| Раздел 7 | 1 | Теория систем с совершенной секретностью. Шифр Вернама. | 4 |
| | 2 | Элементы теории информации. Расстояние единственности шифра с секретным ключом. Идеальные криптосистемы. | 4 |
| | 3 | Современные блоковые и поточные шифры. Криптографические хеш-функции. | 8 |
| | | **Итого по разделу часов** | **16** |
| | | **Всего** | **88** |
| | | **Контроль** | **4** |
| | | **ИТОГО:** | **92** |

**Вид занятий:** лекция, практическая работа, самостоятельная работа и другие.
**Учебно– наглядные пособия:** плакат, стенд, карточки с заданиями, раздаточный материал, методическое пособие, методические рекомендации.

## 5. Примерная тематика курсовых проектов (работ)

Учебным планом не предусмотрены

## 6. Учебно- методическое и информационное обеспечение дисциплины (модуля)

### *6.1 Обеспеченность обучающихся учебниками, учебными пособиями*

| № п/п | Наименование учебника, учебного пособия | Автор | Год издания | Ко-во экземпляров | Электронная версия | Место Размещения электронной версии |
|---|---|---|---|---|---|---|
| Основная литература | | | | | | |
| 1 | Панясенко С. П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. — 576 с | Панясенко С. П. | 2009 | | эл. версия | Кафедра |
| 2 | Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. - М.; ИД -ФОРУМ.: ИНФРА-М, 2008. - 416 с: ил. — (Профессиональное образование). | Шаньгин В. Ф. | 2008 | | эл. версия | Кафедра |

| № п/п | Наименование учебника, учебного пособия | Автор | Год издания | Ко-во экземпляров | Электронная версия | Место Размещения электронной версии |
|---|---|---|---|---|---|---|
| Дополнительная литература | | | | | | |
| 3 | Смарт Н. Криптография.- М.: Техносфера, 2005.-528с | Смарт Н. | 2005 | | эл. версия | Кафедра |
| 4 | Фомичев В.М. Дискретная математика и криптология.- М:ДИАЛОГ-МИФИ, 2003 – 400с. | Фомичев В.М. | 2003 | | эл. версия | Кафедра |
| 5 | Вельшенбах М. Криптография на С и С++ в действии.- М:2004 – 404с | Вельшенбах М. | 2004 | | эл. версия | Кафедра |
| 6 | Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография.-СПб:2004.- 480с. | Ростовцев А.Г., Маховенко Е.Б. | 2004 | | эл. версия | Кафедра |
| 7 | Фергюсон Н., Шнайер Б. Практическая криптография.-М:Вильямс, 2005.- 424с. | Фергюсон Н., Шнайер Б. | 2005 | | эл. версия | Кафедра |
| 8 | Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С, 2-е изд. 2003 г. | Шнайер Б. | 2003 | | эл. версия | Кафедра |
| *Итого по дисциплине: 0% печатных изданий; 100 % электронных* | | | | | | |

### *6.2. Программное обеспечение и Интернет- ресурсы*

Программное обеспечение: *ОС Windows,*

Интернет-ресурсы

Программное обеспечение: ОС Windows, Интегрированный пакет MS Visual Studio; SQL Server,

Интернет-ресурсы: alleng.ru, intuit.ru.

### *6.3. Методические указания и материалы по видам занятий*

Методические указания к лабораторным работам по дисциплине «Криптографические методы защиты информации» в электронном варианте**.**

## ВОПРОСЫ К ЗАЧЕТУ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ "Криптографические методы защиты информации"

1. Арифметика остатков. Группы и кольца. Функция Эйлера. Мультипликативные обратные по модулю $N$. Конечные поля.
2. Алгоритм Евклида.
3. Быстрые алгоритмы возведения в степень.
4. Односторонние функции. Дискретное логарифмирование.
5. Система Диффи-Хеллмана.
6. Шифр Шамира.
7. Шифр Эль-Гамаля.
8. Шифр RSA.
9. Метод «Шаг младенца, шаг великана».
10. Алгоритм исчисления порядка.
11. Электронная подпись RSA.
12. Электронная подпись на базе шифра Эль-Гамаля.
13. Стандарты на цифровую подпись.
14. Ментальный покер.
15. Доказательства с нулевым знанием.
16. Электронные деньги.
17. Взаимная идентификация с установлением ключа.
18. Математические основы эллиптических кривых.. Выбор параметров кривых.
19. Построение криптосистем на эллиптических кривых.
20. Эффективная реализация операций.
21. Определение количества точек на кривой.
22. Использование стандартных кривых
23. Теория систем с совершенной секретностью. Шифр Вернама.
24. Элементы теории информации. Расстояние единственности шифра с секретным ключом.
25. Идеальные криптосистемы.
26. Современные блоковые и поточные шифры.
27. Криптографические хеш-функции.

**7.Материально- техническое обеспечение дисциплины:**

Лаборатория ИТО ИТИ

**8. Методические рекомендации по организации изучения дисциплины:**

Обучающийся, изучающий дисциплину, должен, с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины обучающийся должен знать основные определения, понятия, основные аспекты программной инженерии.

Успешное освоение курса требует самостоятельной работы обучающихся. В программе курса отведено минимально необходимое время для работы обучающихся над темой. Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы;
- проработку учебного материала (по конспектам занятий, учебной и научной литературе), подготовку ответов на вопросы, предназначенные для самостоятельного изучения, доказательство отдельных утверждений, свойств, решение задач;
- подготовка к экзамену.

Руководство и контроль над самостоятельной работой обучающихся осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов следует обращаться за консультациями к лектору.

**9. Технологическая карта дисциплины**

Курс 1

Группа **ИТ22ДР68ИС**

семестр 2

Преподаватель – лектор Бордя Т.Д.

Преподаватели, ведущие лабораторные, практические занятия – БордяТ.Д..

Кафедра «Информационные технологии и автоматизированное управление производственными процессами»

| Наименование дисциплины/курса | Уровень образования (бакалавриат, специалитет, магистратура) | Статус дисциплины в учебном плане (А, Б) | Количество зачетных единиц |
|---|---|---|---|
| Криптографические методы защиты информации | магистратура | | 3 |
| **СМЕЖНЫЕ ДИСЦИПЛИНЫ ПО УЧЕБНОМУ ПЛАНУ:** | | | |
| Научно-исследовательская работа, практика | | | |
| **БАЗОВЫЙ МОДУЛЬ** (проверка знаний и умений по дисциплине) | | | |

| Тема, задание или мероприятие текущего контроля | Виды текущей аттестации | Аудиторная или внеаудиторная | Минимальное количество баллов | Максимальное количество баллов |
|---|---|---|---|---|
| Лабораторная работа №1 | ЛР1 | Аудиторная | 8 | 16 |
| Лабораторная работа №2 | ЛР2 | Аудиторная | 8 | 16 |
| Лабораторная работа №3 | ЛР3 | Аудиторная | 8 | 16 |
| **РУБЕЖНЫЙ КОНТРОЛЬ** | **РК** | | **24** | **48** |
| Лабораторная работа №4 | ЛР4 | Аудиторная | 6,5 | 13 |
| Лабораторная работа №5 | ЛР5 | Аудиторная | 6,5 | 13 |
| Лабораторная работа №6 | ЛР6 | Аудиторная | 6,5 | 13 |
| Лабораторная работа №7 | ЛР7 | Аудиторная | 6,5 | 13 |
| **РУБЕЖНАЯ АТТЕСТАЦИЯ** | **РА** | | **26** | **52** |
| | | **Итого** | **50** | **100** |

Рабочая учебная программа рассмотрена методической комиссией инженерно-технического института протокол №1 от «30» 09 2022 г. и признана соответствующей требованиям Государственного образовательного стандарта и учебного плана по направлению 2.09.04.02 Информационные системы и технологии.

Председатель МК ИТИ Е.А. Царюк