Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный
университет имени
Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«27» 06 2025 г.
Регистрационный № УД-3857/25/уч

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения образования
по учебной дисциплине для специальности
6-05-0533-12 «Кибербезопасность»

2025 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 6-05-0533-12-2023 и учебного плана специальности 6-05-0533-12 «Кибербезопасность». Регистрационный 14-23/уч. ФКНЭ от 04.04.2023 для дневной формы получения высшего образования

СОСТАВИТЕЛЬ:
Сергей Васильевич Кухта, старший преподаватель кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕЦЕНЗЕНТЫ:
Валерий Михайлович Чертков, заведующий кафедрой технологий программирования учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
Константин Яковлевич Раханов, технический директор ООО «ТриИнком», к.т.н, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 6 от «30» 05 2025 г.)

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 7 от «27» 06 2025 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Криптографические методы защиты информации обеспечивают конфиденциальность, контроль целостности и проверку подлинности данных с помощью ключезависимых или бесключевых криптографических преобразований.

Учебная дисциплина «Криптографические методы защиты информации» знакомит студентов с методами построения криптографических преобразований, а также методами оценки их надежности. Кроме того, данная учебная дисциплина дает представление об основных типах криптографических систем: симметричных, блочных, поточных, криптосистемах с открытым ключом, систем электронной цифровой подписи, функций хеширования.

Изучаемые криптографические методы основываются на использовании объектов и применении методов широкого набора математических дисциплин: алгебры, теории чисел, теории вероятностей, математической статистики, теории информации, теории сложности.

Цели изучения учебной дисциплины «Криптографические методы защиты информации»: дать студентам теоретические основы построения надежных криптографических преобразований, сформировать навыки использования криптографических преобразований для построения систем защиты информации.

При изложении материала учебной дисциплины важно показать возможности использования конкретных криптографических методов при решении прикладных задач защиты информации.

З***адачи***, решаемые при изучении учебной дисциплины «Криптографические методы защиты информации»:

– изучение криптосистем с секретным ключом, применение блочных и поточных криптосистем для решения практических задач в области защиты информации;

– изучение криптосистем с открытым ключом, применение функций хеширования для решения задач проверки целостности сообщений, использование электронной цифровой подписи;

– изучение основ применения эллиптических кривых в криптографии.

При изучении дисциплины «Криптографические методы защиты информации» у студентов специальности 6-05-0533-12 «Кибербезопасность» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «Специалист по кибербезопасности», обеспечивающих выпускникам успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

универсальные компетенции

- Владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации.

- Решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий.

- Работать в команде, толерантно воспринимать социальные, этнические, конфессиональные и межкультурные взаимодействия.

- Быть способным к саморазвитию и совершенствованию в профессиональной деятельности.

- Проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности.

базовые профессиональные компетенции

- Использовать основные понятия и нормативные правовые акты в сфере кибербезопасности для описания, классификации и применения теоретических, нормативно-правовых, инженерно-технических, организационных методов обеспечения безопасности информации и информационно-коммуникационных инфраструктур.

В результате освоения учебной дисциплины студент должен:

знать:

– методы построения надежных блочных и поточных криптосистем, функций хеширования, криптосистем с открытым ключом и систем электронной цифровой подписи;

– задачи и основные методы криптоанализа;

– стандартные криптосистемы и их практическое использование;

уметь:

– применять полученные знания для создания надежных систем защиты информации;

владеть:

– методами построения надежных криптосистем и функций хеширования;

– методами построения криптосистем с открытым ключом и систем электронной цифровой подписи;

– основными методами криптоанализа.

Связи с другими учебными дисциплинами.

Основой для изучения учебной дисциплины «Криптографические методы защиты информации» по специальности 6-05-0533-12 «Кибербезопасность» являются учебные дисциплины «Аналитическая геометрия и линейная алгебра», «Дискретная математика и математическая логика», «Теория вероятностей и математическая статистика», «Основы кибербезопасности».

Знания, полученные при изучении учебной дисциплины «Криптографические методы защиты информации», являются основой для дипломного проектирования, используются учебными дисциплинами «Криптографические протоколы», «Криптографический инжиниринг», «Методы и стандарты оценки защищенности компьютерных систем».

Форма получения высшего образования – дневная.

В соответствии с учебным планом по специальности 6-05-0533-12 «Кибербезопасность» на изучение учебной дисциплины отводится:

Форма получения высшего образования	дневная
Курс (курсы)	3
Семестр	5
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	62
В том числе:	
Лекций, часов	34
Лабораторные занятия, часов	28
Самостоятельная работа, часов	46
Форма промежуточной аттестации	зачет
Трудоемкость дисциплины, зачетные единицы	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. КРИПТОГРАФИЯ С СЕКРЕТНЫМ КЛЮЧОМ

Тема 1.1. Введение в криптографию.

История криптографии. Абоненты, коммуникации и угрозы. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы). Типы атак. Сложность атак.

Тема 1.2. Классические криптосистемы.

Шифры перестановки. Шифр сдвига. Шифры простой замены. Аффинный шифр. Шифры многоалфавитной замены. Шифр Хилла. Шифр Виженера.

Тема 1.3. Элементы теории Шеннона.

Совершенные криптосистемы. Энтропия, условная энтропия, удельная энтропия. Расстояние единственности.

Тема 1.4. Блочные криптосистемы.

Блочно-итерационные криптосистемы. SP-криптосистемы. AES. Использование инволютивных подстановок. Криптосистемы Фейстеля. Атака «грубой силой». Баланс «время-память». Таблицы разностей. Разностная атака. Конструкция Нюберг. Линейные аппроксимации. Линейная атака. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью.

Тема 1.5. Свойства линейных рекуррентных последовательностей.

Порядок многочлена. Примитивные многочлены. Период л.р.п. Минимальный многочлен. Постулаты Голомба.

Тема 1.6. Поточные криптосистемы.

Конечные автоматы. Регистры сдвига с линейной обратной связью. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Криптосистема A5/1. Сжимающий и самосжимающий генератор. Линейная сложность. Корреляционный криптоанализ. Корреляционно-иммунные функции.

Раздел 2. КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Тема 2.1. Протокол Диффи-Хеллмана.

Идея криптографии с открытым ключом. Головоломки Меркля. Протокол Диффи-Хеллмана. Реализация протокола Диффи-Хеллмана.

Тема 2.2. Элементы теории сложности.

Вычислительные проблемы. Машины Тьюринга. Предикаты. Классы сложности. Вероятностные машины. Алгоритмы типа Монте-Карло и Лас-Вегас. Односторонние функции. Функция Рабина. Функции с лазейкой. Лазейка функции Рабина. Функция RSA. Функция ЭльГамаля.

Тема 2.3. Криптосистемы с открытым ключом.

Использование функций с лазейкой для построения криптосистем с открытым ключом. Криптосистема RSA. RSA и факторизация. Реализация: арифметика больших чисел, алгоритм Евклида, возведение в степень, оптимизация RSA. Криптосистема Рабина. Криптосистема ЭльГамаля.

Тема 2.4. Генерация простых чисел.

Язык PRIMES. Проверка простоты. Тесты Ферма и Миллера-Рабина. Построение простых чисел. Теорема Диемитко.

Тема 2.5. Функции хеширования.

Определения и задачи криптоанализа. Использование. Генераторы псевдослучайных чисел на базе функций хеширования. Ключезависимые функции хеширования. Блочно-итерационные функции хеширования. Функция хеширования СТБ 34.101.31. Атака «дней

рождения». Алгоритм Брента.

Тема 2.6. Электронные цифровые подписи.

Использование функций с лазейкой для построения систем ЭЦП. ЭЦП Эль-Гамаля. Реализация ЭЦП Эль-Гамаля. ЭЦП Шнорра. Система ЭЦП СТБ 1176.2.

Тема 2.7. Факторизация и дискретное логарифмирование.

Алгоритм р - 1. р-методы. Выбор модуля RSA. Метод больших-малых шагов. л-метод. Метод Поллига-Хеллмана. Алгоритм Диксона. Квадратичное решето. Индекс-метод.

Тема 2.8. Эллиптические кривые в криптографии.

Основные понятия. Сложение точек. Кривые над конечными полями. Кратная точка. ЭЦП Шнорра на эллиптических кривых. Система ЭЦП СТБ 34.101.45.

Учебно-методическая карта учебной дисциплины «Криптографические методы защиты информации»
Дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		Лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
Раздел 1	**Криптография с секретным ключом**	**12**	**12**				
Тема 1.1	***Введение в криптографию.*** История криптографии. Абоненты, коммуникации и угрозы. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы). Типы атак. Сложность атак.	2				Осн. лит.: [1], [4]. Доп. лит.: [1], [2].	Блиц-опрос
Тема 1.2	***Классические криптосистемы.*** Шифры перестановки. Шифр сдвига. Шифры простой замены. Аффинный шифр. Шифры многоалфавитной замены. Шифр Хилла. Шифр Виженера.	2				Осн. лит.: [1], [4]. Доп. лит.: [2].	Блиц-опрос
	Лабораторная работа №1. Исследование классических криптосистем.		2			Методические указания	Защита отчета по лабораторной работе
Тема 1.3	***Элементы теории Шеннона.*** Совершенные криптосистемы. Энтропия, условная энтропия, удельная энтропия. Расстояние единственности.	2				Осн. лит.: [1], [4]. Доп. лит.: [2].	Блиц-опрос
Тема 1.4	***Блочные криптосистемы.*** Использование инволютивных подстановок. Криптосистемы Фейстеля. Блочно-итерационные криптосистемы. SP-криптосистемы. AES.	2				Осн. лит.: [1], [3], [4]. Доп. лит.: [2], [3].	Контрольное тестирование №1
	Лабораторная работа №2. Исследование криптосистем Фейстеля.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №3. Исследование блочно-итерационных криптосистем.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №4. Исследование SP-криптосистем.		2			Методические указания	Защита отчета по лабораторной работе

1	2	3	4	5	6	7	8
Тема 1.5	***Свойства линейных рекуррентных последовательностей.*** Порядок многочлена. Примитивные многочлены. Период л.р.п. Минимальный многочлен. Постулаты Голомба.	2				Осн. лит.: [2], [3]. Доп. лит.: [2].	Блиц-опрос
	Лабораторная работа №5. Анализ генераторов псевдослучайной последовательности.		2			Методические указания	Защита отчета по лабораторной работе
Тема 1.6	***Поточные криптосистемы.*** Конечные автоматы. Регистры сдвига с линейной обратной связью. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Криптосистема A5/1. Сжимающий и самосжимающий генератор.	2				Осн. лит.: [1], [3], [4]. Доп. лит.: [2], [3].	Блиц-опрос
	Лабораторная работа №6. Исследование поточных криптосистем.		2			Методические указания	Защита отчета по лабораторной работе
Раздел 2	**Криптография с открытым ключом.**	**22**	**16**				
Тема 2.1	***Протокол Диффи-Хеллмана.*** Идея криптографии с открытым ключом. Головоломки Меркля. Протокол Диффи-Хеллмана. Реализация протокола Диффи-Хеллмана.	2				Осн. лит.: [1], [3], [5]. Доп. лит.: [1], [2].	Контрольное тестирование №2
	Лабораторная работа №7. Программная реализация протокола Диффи-Хеллмана.		2			Методические указания	Защита отчета по лабораторной работе
Тема 2.2	***Элементы теории сложности.*** Вычислительные проблемы. Машины Тьюринга. Предикаты. Классы сложности. Вероятностные машины. Алгоритмы типа Монте-Карло и Лас-Вегас. Односторонние функции. Функция Рабина. Функции с лазейкой. Лазейка функции Рабина.	2				Осн. лит.: [2], [4]. Доп. лит.: [2].	Блиц-опрос
Тема 2.3	***Криптосистемы с открытым ключом.*** Использование функций с лазейкой для построения криптосистем с открытым ключом. Криптосистема RSA. RSA и факторизация. Реализация: арифметика больших чисел, алгоритм Евклида, возведение в степень, оптимизация RSA.	2				Осн. лит.: [1], [2]. Доп. лит.: [2], [3].	Блиц-опрос
	Криптосистема Рабина. Криптосистема Эль-Гамаля. Стойкость криптосистем.	2					
	Лабораторная работа №8. Исследование криптосистем с открытым ключом.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №8. Исследование криптосистем с открытым ключом.		2				

1	2	3	4	5	6	7	8
Тема 2.4	***Генерация простых чисел.*** Язык PRIMES. Проверка простоты. Тесты Ферма и Миллера-Рабина. Построение простых чисел. Теорема Диемитко.	2				Осн. лит.: [1], [2], [5]. Доп. лит.: [2], [3].	Блиц-опрос
	Лабораторная работа №9. Исследование генератора простых чисел.		2			Методические указания	Защита отчета по лабораторной работе
Тема 2.5	***Функции хеширования.*** Определения и задачи криптоанализа. Использование. Генераторы псевдослучайных чисел на базе функций хеширования. Ключезависимые функции хеширования.	2				Осн. лит.: [1], [2], [5]. Доп. лит.: [2], [3].	Блиц-опрос
	Блочно-итерационные функции хеширования. Функция хеширования СТБ 34.101.31. Атака «дней рождения». Алгоритм Брента.	2					
	Лабораторная работа №10. Программная реализация функций хеширования.		2			Методические указания	Защита отчета по лабораторной работе
Тема 2.6	***Электронные цифровые подписи.*** Использование функций с лазейкой для построения систем ЭЦП. ЭЦП Эль-Гамаля. Реализация ЭЦП Эль-Гамаля. ЭЦП Шнорра. Система ЭЦП СТБ 1176.2.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [2].	Контрольное тестирование №3
	Лабораторная работа №11. Программная реализация алгоритмов электронной цифровой подписи.		2			Методические указания	Защита отчета по лабораторной работе
Тема 2.7	***Тема 2.8. Факторизация и дискретное логарифмирование.*** Алгоритм р - 1. р-методы. Выбор модуля RSA. Метод больших-малых шагов. л-метод. Метод Поллига-Хеллмана. Алгоритм Диксона. Квадратичное решето. Индекс-метод.	2				Осн. лит.: [1], [2], [5]. Доп. лит.: [2], [3].	Блиц-опрос
	Лабораторная работа №12. Анализ алгоритмов факторизации.		2			Методические указания	Защита отчета по лабораторной работе

1	2	3	4	5	6	7	8
Тема 2.8	***Эллиптические кривые в криптографии.*** Основные понятия. Сложение точек. Кривые над конечными полями. Кратная точка.	2				Осн. лит.: [1], [3], [5]. Доп. лит.: [2], [3].	Контрольное тестирование №4
	ЭЦП Шнорра на эллиптических кривых. Система ЭЦП СТБ 34.101.45.	2					
	Лабораторная работа №13. Использование эллиптических кривых в криптоалгоритмах.		2			Методические указания	Защита отчета по лабораторной работе
	Всего	**34**	**28**				

Примечание: в соответствии с рейтинговой системой для определения результата текущего контроля за семестр в виде отметки в баллах по десятибалльной шкале используются отметки, полученные за мероприятия текущего контроля в течение семестра, обозначенные в графе «Форма контроля знаний»

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Васильева, И.Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. – Москва: Юрайт, 2023. – 349 с. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника и практикума для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

2. Деза, Е.И. Введение в криптографию. Теоретико-числовые основы защиты информации: учебное пособие / Е. И. Деза, Л. В. Котова. - издание стереотипное. – Москва : ЛЕНАНД, 2022. – 368 с. – (Основы защиты информации. № 14).

3. Романьков, В.А. Введение в криптографию: курс лекций / В. А. Романьков. – 2 издание, исправленное и дополненное. – Москва: ИНФРА-М, 2023. – 234 с. – Рекомендовано в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки 01.03.01 «Математика», 02.03.01 «Математика и компьютерные технологии», 01.03.02 «Прикладная математика и информатика» (квалификация (степень) «бакалавр»).

4. Фомичев, В.М. Криптографические методы защиты информации: учебник для вузов: в 2 частях / В. М. Фомичев, Д. А. Мельников; под редакцией В.М. Фомичева. – Москва: Юрайт, 2023. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям. Часть 1 : Математические аспекты. – 2023. – 209 с.

5. Фомичев, В.М. Криптографические методы защиты информации: учебник для вузов: в 2 частях / В. М. Фомичев, Д. А. Мельников; под редакцией В.М. Фомичева. – Москва: Юрайт, 2023. – (Высшее образование). – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям. Часть 2: Системные и прикладные аспекты. – 2023. – 245 с. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

Дополнительная:

1. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург : Лань, 2020. – 124 с. – ISBN 978-5-8114-4404-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/133924 (дата обращения: 19.08.2022). – Режим доступа: для авториз. пользователей.

2. Криптология: учебник / Харин Ю. С. [и др.] - Минск : БГУ, 2013. – 511 с. – (Классическое университетское издание).

3. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 577 с. – Текст : электронный.

Гущова Е. В

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа №1 Исследование классических криптосистем.

Лабораторная работа №2 Исследование криптосистем Фейстеля.

Лабораторная работа №3 Исследование блочно-итерационных криптосистем.

Лабораторная работа №4 Исследование SP-криптосистем.

Лабораторная работа №5 Анализ генераторов псевдослучайной последовательности.

Лабораторная работа №6 Исследование поточных шифров.

Лабораторная работа №7 Программная реализация протокола Диффи-Хеллмана.

Лабораторная работа №8 Исследование криптосистем с открытым ключом.

Лабораторная работа №9 Исследование генератора простых чисел.

Лабораторная работа №10 Программная реализация функций хеширования.

Лабораторная работа №11 Программная реализация алгоритмов электронной цифровой подписи.

Лабораторная работа №12 Анализ алгоритмов факторизации.

Лабораторная работа №13 Использование эллиптических кривых в криптоалгоритмах.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

1. Определения криптологии, криптографии, криптоанализа. Назначение криптографии. Криптозащита данных. Шифр. Алфавит сообщений. Процесс шифрования/расшифрования. Основное требования к шифру. Ключ. Криптостойкость шифра. Криптографические ключи. Электронная цифровая подпись.
2. Модель канала передачи данных, обеспечивающая секретность. Криптографическая система. Правило техники криптографического кодирования. Схема асимметричной криптосистемы. Требования к криптосистемам. Безопасность криптосистем.
3. Схема симметричной криптосистемы. Классификация симметричных криптосистем.
4. Идея шифра перестановки. Простая перестановка: ключ, шифрование, расшифрование.
5. Одиночная перестановка по ключу: ключ, шифрование, расшифрование. Двойная перестановка: ключ, шифрование, расшифрование. Магический квадрат: ключ, шифрование, расшифрование. Шифр Кардано: ключ, шифрование, расшифрование. Шифр Ришелье: ключ, шифрование, расшифрование.
6. Полибианский квадрат: ключ, шифрование, расшифрование. Шифр Цезаря: ключ, шифрование, расшифрование, криптостойкость. Шифр Цезаря с ключевым словом: ключ, шифрование, расшифрование, криптостойкость. Аффинная система подстановок Цезаря: ключ, шифрование, расшифрование, криптостойкость. Шифр Плейфера: ключ, шифрование, расшифрование, криптостойкость. Шифр Хилла: ключ, шифрование, расшифрование, криптостойкость.
7. Многоалфавитные шифры замены. Диск Альберти: ключ, шифрование, расшифрование. Шифр Гронсфельда: ключ, шифрование, расшифрование. Шифр Вижинера: ключ, шифрование, расшифрование. Одноразовый блокнот: ключ, шифрование, расшифрование, криптостойкость. Двойной квадрат Уитстона: ключ, шифрование, расшифрование.
8. Псевдослучайная последовательность. Генератор псевдослучайной последовательности. Классификация алгоритмов генерации. Линейный конгруэнтный генератор. Мультипликативный конгруэнтный генератор. Квадратичный конгруэнтный генератор. Генератор Эйхенауэра-Лена. Конгруэнтный генератор, использующий умножение с переносом. Рекурренты в конечном поле. LFSR-генератор. Генератор Таусворта. Генератор Фибоначчи. Метод Макларена-Марсальи.
9. Гамма шифра. Ключ шифра с гаммированием. Гаммирование с конечной и бесконечной гаммой. Процесс шифрования гаммированием. Процесс расшифрования гаммированием. Криптостойкость шифра с гаммированием.
10. Потоковый шифр. Последовательность выбора шифрпреобразований в потовых шифрах. Принцип работы потокового шифра. Достоинства и недостатки потокового шифра.
11. Требования к современным криптосистемам. Определение блочного шифра. Ключевая система блочных шифров. Возможности злоумышленника по взлому блочных шифров. Определение сети Фейстела. Структура итерации сети Фейстела. Достоинства и недостатки шифров на основе сети Фейстела.
12. Достоинства и недостатки криптосистемы DES. Обобщенная схема шифрования в криптосистеме DES. Шаги алгоритмов шифрования и расшифрования DES. Схема алгоритма вычисления ключей для раундов DES. Криптостойкость DES. Режимы работы DES. Алгоритм тройной DES. Алгоритм расширение DES.
13. Характеристика алгоритма Rijndael. Шаги алгоритма Rijndael: блок нелинейной обратимой байтовой замены; циклический сдвиг влево строк массива; перемешивание столбцов; добавление ключа итерации. Принципы построения ключа итерации. Стойкость алгоритма Rijndael. Характеристика алгоритма RC6.
14. Сравнение DES и ГОСТ 28147-89. Характеристика алгоритма ГОСТ 28147-89. Схема алгоритма ГОСТ 28147-89. Режимы работы алгоритма ГОСТ 28147-89. Стойкость алгоритма ГОСТ 28147-89. Сравнение DES и ГОСТ 28147-89. Сравнение ГОСТ 28147-89 и Rijndael.

15. Общая схема криптосистемы по Шеннону. Математическая модель криптосистем: подстановки; перестановки с периодом T; шифра Виженера; шифра Цезаря; шифра Бофора; Вернама; биграмной подстановки.
16. Совершенно криптостойкая симметричная криптосистема. Необходимое и достаточное условие совершенной криптостойкости симметричной криптосистемы. Условие совершенной криптостойкости криптопреобразования Вернама. Расстояние единственности.
17. Гамма шифра. Ключ шифра с гаммированием. Гаммирование с конечной и бесконечной гаммой. Процесс шифрования гаммированием. Процесс расшифрования гаммированием. Криптостойкость шифра с гаммированием.
18. Потоковый шифр. Последовательность выбора шифрпреобразований в потовых шифрах. Принцип работы потокового шифра. Достоинства и недостатки потокового шифра.
19. Требования к современным криптосистемам. Определение блочного шифра. Ключевая система блочных шифров. Возможности злоумышленника по взлому блочных шифров.
20. Определение сети Фейстела. Структура итерации сети Фейстела. Достоинства и недостатки шифров на основе сети Фейстела.
21. Достоинства и недостатки криптосистемы DES. Обобщенная схема шифрования в криптосистеме DES. Шаги алгоритмов шифрования и расшифрования DES. Схема алгоритма вычисления ключей для раундов DES. Криптостойкость DES. Режимы работы DES. Алгоритм тройной DES. Алгоритм расширение DES.
22. Характеристика алгоритма Rijndael. Шаги алгоритма Rijndael: блок нелинейной обратимой байтовой замены; циклический сдвиг влево строк массива; перемешивание столбцов; добавление ключа итерации. Принципы построения ключа итерации. Стойкость алгоритма Rijndael. Характеристика алгоритма RC6.
23. Характеристика алгоритма ГОСТ 28147-89. Схема алгоритма ГОСТ 28147-89. Режимы работы алгоритма ГОСТ 28147-89. Стойкость алгоритма ГОСТ 28147-89. Сравнение DES и ГОСТ 28147-89. Сравнение ГОСТ 28147-89 и Rijndael.
24. Общая схема криптосистемы по Шеннону. Математическая модель криптосистем: подстановки; перестановки с периодом T; шифра Виженера; шифра Цезаря; шифра Бофора; Вернама; биграмной подстановки.
25. Совершенно криптостойкая симметричная криптосистема. Необходимое и достаточное условие совершенной криптостойкости симметричной криптосистемы. Условие совершенной криптостойкости криптопреобразования Вернама. Расстояние единственности.
26. Понятие асимметричной криптосистемы. Теоретические основы асимметричных криптосистем: однонаправленная функция с секретом. Нестойкость «учебных» алгоритмов шифрования. Сравнительная характеристика симметричных и асимметричных шифров
27. Предыстория и основные идеи асимметричных криптосистем. Открытое распределение криптографических ключей. Схема Диффи-Хеллмана. Атака «человек посередине» на протокол Диффи-Хеллмана. Задача Диффи-Хеллмана и задача дискретного логарифмирования
28. Криптосистема RSA. Взлом криптосистем с открытым ключом с помощью криптоанализа. Задача RSA. Разложение целых чисел на простые множители. Уязвимость «учебного» криптоалгоритма RSA
29. Криптосистема Рабина. Уязвимость «учебного» криптоалгоритма Рабина
30. Криптосистема Эль-Гамаля. Уязвимость «учебного» криптоалгоритма Эль-Гамаля. Атака «встреча посередине» и активная атака на учебную криптосистему Эль-Гамаля
31. Необходимость понятия повышенной стойкости для криптосистем с открытым ключом
32. Комбинация асимметричной и симметричной криптографии
33. Функции хеширования и целостность данных. Типы криптографических хеш-функций. Алгоритмы хеш-функций

34. Обобщенная модель электронной цифровой подписи. Цифровые подписи, основанные на асимметричных криптосистемах. Стандарт цифровой подписи DSS. Цифровые подписи, основанные на симметричных криптосистемах. Слепая подпись Чаума
35. Элементы теории эллиптических кривых над конечными полями. Задание криптосистемы над эллиптическими кривыми. Обобщение криптосистемы Эль-Гамаля на случай эллиптических кривых

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Криптографические методы защиты информации» предполагает реализацию следующих форм самостоятельной работы студентов:

– проработка конспекта лекций и учебной литературы;

– изучение печатных источников по теме дисциплины;

– изучение профессиональных электронных ресурсов по теме дисциплины;

– изучение вопросов для самоконтроля;

– подготовка к аудиторному выполнению лабораторных работ (предварительное знакомство с методическими указаниями, вариантом индивидуального задания по работе);

– решение индивидуальных задач при подготовке к лабораторным занятиям;

–подготовка к защите лабораторных работ (оформление отчёта по индивидуальному варианту задания, защита результатов работы и демонстрации степени освоения навыков и умений по конкретной теме);

–углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;

– изучение основной и дополнительной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;

–систематизация полученных знаний при подготовке к зачету.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации образовательного процесса, обеспечиваются:

– наличием и использованием в образовательном процессе учебного курса по дисциплине «Криптографические методы защиты информации» в системе дистанционного обучения Moodle для доступа студентов к электронным вариантам курса лекций и учебно-методических указаний по основным разделам дисциплины, для организации учебной деятельности студентов и контроля ее результативности.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Учебный курс по дисциплине «Криптографические методы защиты информации» в системе дистанционного обучения Moodle (ссылка https://moodle.psu.by/course/view.php?id=268).

2. Методические указания к выполнению лабораторных работ по дисциплине «Криптографические методы защиты информации» для студентов специальности 6-05-0533-12 «Кибербезопасность».

Содержание самостоятельной работы студентов

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	*Тема 1.3. Элементы теории Шеннона.* Энтропия, условная энтропия, удельная энтропия. Расстояние единственности. Осн. лит.: [1], [4]. Доп. лит.: [2].	1
	Тема 1.4. Блочные криптосистемы. Использование инволютивных подстановок. Криптосистемы Фейстеля.Блочно-итерационные криптосистемы. SP-криптосистемы. AES. Атака «грубой силой». Баланс «время-память». Таблицы разностей. Разностная атака. Конструкция Нюберг. Линейные аппроксимации. Линейная атака. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью. Осн. лит.: [1], [3], [4]. Доп. лит.: [2], [3].	4
	Тема 1.6. Поточные криптосистемы. Конечные автоматы. корреляционный криптоанализ. Корреляционно-иммунные функции. Осн. лит.: [1], [3], [4]. Доп. лит.: [2], [3].	2
	Тема 2.3. Криптосистемы с открытым ключом. Реализация: арифметика больших чисел, алгоритм Евклида, возведение в степень. Осн. лит.: [1], [2], [5]. Доп. лит.: [2], [3].	3
	Тема 2.8. Эллиптические кривые в криптографии. Сложение точек. Кривые над конечными полями. Кратная точка. Осн. лит.: [1], [3], [5]. Доп. лит.: [2], [3].	3
Подготовка к защите отчетов по лабораторным работам	*Лабораторная работа №1* Исследование классических криптосистем.	2
	Лабораторная работа № 2 Исследование криптосистем Фейстеля.	3
	Лабораторная работа №3 Исследование блочно-итерационных криптосистем.	3
	Лабораторная работа №4 Исследование SP-криптосистем.	3
	Лабораторная работа №5 Анализ генераторов псевдослучайной последовательности.	2
	Лабораторная работа №6 Исследование поточных шифров.	2
	Лабораторная работа №7 Программная реализация протокола Диффи-Хеллмана.	2
	Лабораторная работа №8 Исследование криптосистем с открытым ключом.	3
	Лабораторная работа №9 Исследование генератора простых чисел.	2
	Лабораторная работа №10 Программная реализация функций хеширования.	3
	Лабораторная работа №11 Программная реализация алгоритмов электронной цифровой подписи	3

1	2	3
	Лабораторная работа №12 Анализ алгоритмов факторизации.	2
	Лабораторная работа №13 Использование эллиптических кривых в криптоалгоритмах.	3
		46

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Контроль качества усвоения знаний проводится в форме текущего контроля и промежуточной аттестации.

Мероприятия текущего контроля проводятся в течение семестра и включают в себя следующие **формы контроля:**

–устная форма (блиц-опрос на лекциях);

–письменная форма (тесты, письменные отчёты по лабораторным работам);

–устно-письменная форма (отчёты по лабораторным работам с их устной защитой);

–техническая форма (электронные тесты).

Лабораторные работы предполагают выполнение и защиту. При их выполнении выдаётся индивидуальное задание. Отчёт по лабораторной работе представляется в электронном виде. Содержание отчёта: название работы, вариант задания, анализ задания, ход выполнения работы, основные и промежуточные результаты, выводы по работе. Защита работ проводится индивидуально и оценивается в соответствии с установленными правилами.

Результат текущего *контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится исходя из отметок, выставленных в ходе проведения мероприятий текущего контроля в течение семестра по следующей формуле:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_{n1}) + (\text{ЛР}_1 + \cdots + \text{ЛР}_{n2}) + (\text{УО}_1 + \cdots + \text{УО}_{n3})}{(17 + n)},$$

где $\text{КТ}_1, \ldots, \text{КТ}_{n1}$ – отметки, выставленные по результатам контрольного тестирования; $n1$ – количество тестов; $\text{ЛР}_1, \ldots, \text{ЛР}_{n2}$ – отметки, выставленные по результатам защит лабораторных работ; $n2$ – количество работ; УО_1, ..., УО_{n3} – отметки, выставленные по результатам устных опросов на лекциях; $n3$ – количество устных опросов.

Результат текущего контроля рассчитывается как округлённое среднее значение.

Для обучающего, пропустившего мероприятие текущего контроля по уважительной причине, кафедрой устанавливаются дополнительные сроки.

Обучающемуся, пропустившему мероприятие текущего контроля без уважительной причины, выставляется 1 (один) балл за данное мероприятие.

Результат текущего контроля может быть повышен:

- за участие обучающего в научно-практических мероприятиях, учебно-исследовательской, научно-исследовательской работе студентов (конференциях, семинарах, олимпиадах, конкурсах, научных кружках и т.п.) по профилю учебной дисциплины (модуля) и может быть повышен до 10 баллов при достижении значимых результатов в этой работе;

- обучающийся в целях повышения отметки по любому мероприятию текущего контроля может воспользоваться правом на дополнительные образовательные услуги (платные консультации, платные дополнительные занятия). Количество и сроки пересдач с целью повышения отметки определяет кафедра.

Промежуточная аттестация проводится в форме зачёта в пятом семестре.

Заключение о *зачёте* формируется по формуле:

$$\text{З} = k \cdot \text{Т},$$

где k – весовой коэффициент текущего контроля; Т – результат текущего контроля за семестр. Весовой коэффициент k принимается равным 1.

Если полученная отметка $\text{З} < 4$ баллов, то проводится устный зачёт отдельно по представленным в программе вопросам.

Перевод отметки по зачету осуществляется по следующим правилам: отметка «зачтено» выставляется студентам, получившим от 4 до 10 баллов, отметка «не зачтено» выставляется студентам, получившим от 1 до 3 баллов.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основные методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

– проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;

– учебно-исследовательская деятельность, реализация творческого подхода, реализуемые на лабораторных занятиях.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Криптографические методы защиты информации» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в чётком понимании им значимости всех видов выполняемых работ, как с точки зрения важности для профессиональной подготовки, так и с точки зрения оценивания. Подход предполагает использование элементов проблемного обучения и элементов исследовательской деятельности студентов в процессе аудиторной работы, а также при выполнении самостоятельных работ при постоянном рейтинговом контроле.

На лекционных занятиях по дисциплине «Криптографические методы защиты информации» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и лабораторных занятиях.

На лекционных занятиях студенты овладевают системой теоретических знаний в области методов криптографической защиты информации. В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий с опорой на имеющуюся начальную подготовку студентов и их математический кругозор, использованием интерактивных методов обучения.

На лабораторных занятиях развиваются и формируются необходимые практические умения и навыки программной реализации криптографических методов защиты информации.

Применяется индивидуальный, творческий подход. Также во время проведения лабораторных работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу
Дипломное проектирование	МиКБ	Предложений и замечаний нет	
Криптографический инжиниринг	МиКБ	Предложений и замечаний нет	
Криптографические протоколы	МиКБ	Предложений и замечаний нет	
Методы и стандарты оценки защищенности компьютерных систем	МиКБ	Предложений и замечаний нет	

Заведующий кафедрой математики и компьютерной безопасности, к.т.н., доцент И. Б. Бураченок

РЕЦЕНЗИЯ
на учебную программу учреждения образования
по учебной дисциплине «Криптографические методы защиты информации»
для специальности 6-05-0533-12 «Кибербезопасность»

Разработчиком учебной программы учреждения образования по учебной дисциплине «Криптографические методы защиты информации» для специальности 6-05-0533-12 «Кибербезопасность» учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» является старший преподаватель кафедры математики и компьютерной безопасности С.В.Кухта.

Программа содержит все необходимые структурные элементы и соответствует требованиям, предъявляемым к документам такого рода. В «Пояснительной записке» отражены цели изучения, принципы и подходы к формированию программы учебной дисциплины, особенности планирования программы. Рецензируемая учебная программа содержит все необходимые для организации учебного процесса по дисциплине «Криптографические методы защиты информации» для специальности 6-05-0533-12 «Кибербезопасность» элементы: цели и задачи дисциплины, требования к уровню освоения содержания учебной дисциплины, соотнесенные с перечнем планируемых результатов обучения, связи данной дисциплины с другими дисциплинами учебного плана специальности, содержание учебного материала, учебно-методическую карту дисциплины, структурированную по темам и разделам с указанием отведенного на них количества академических часов и видов учебных занятий, список основной и дополнительной литературы, перечень вопросов для проведения зачета, описание содержания самостоятельной работы студентов и организации контроля качества усвоения знаний, характеристику подходов к преподаванию учебной дисциплины.

Тематический план учебной дисциплины имеет оптимальное распределение часов по разделам и темам в соответствии с учебным планом. Каждый раздел программы отражает тематику и вопросы, позволяющие в полном объеме изучить необходимый материал с практическим формированием и закреплением умений и навыков на лабораторных занятиях. Материал изложен грамотно, логично, аргументированно.

Предлагаемая к использованию основная и дополнительная литература достаточна и современна, позволит организовать самостоятельную работу студентов при изучении теоретического материала по темам дисциплины, выполнении лабораторных работ.

Подходы к организации контроля качества усвоения знаний обеспечивают объективность и достоверность результатов при проведении текущего контроля и промежуточной аттестации.

Представленная на рецензию учебная программа учреждения образования по учебной дисциплине «Криптографические методы защиты информации» для специальности 6-05-0533-12 «Кибербезопасность» отвечает предъявляемым требованиям и профессиональным задачам образовательной программы высшего образования и может быть использована в учебном процессе.

Рецензент:
Заведующий кафедрой технологий
программирования УО «Полоцкий государственный
университет имени Евфросинии Полоцкой»
к.т.н., доцент В.М. Чертков

РЕЦЕНЗИЯ

на учебную программу учреждения образования
по учебной дисциплине «Криптографические методы защиты информации»
для специальности 6-05-0533-12 «Кибербезопасность»

Разработчиком учебной программы учреждения образования по учебной дисциплине «Криптографические методы защиты информации» для специальности 6-05-0533-12 «Кибербезопасность» УО «Полоцкий государственный университет имени Евфросинии Полоцкой» является старший преподаватель кафедры математики и компьютерной безопасности С.В.Кухта.

Знание теоретических основ построения надежных криптографических преобразований, владение навыками реализации и использования криптографических преобразований для построения систем защиты информации важно для профессиональной деятельности специалиста по защите информации. Дисциплина «Криптографические методы защиты информации» является системообразующей для изучения и качественного освоения ряда специальных дисциплин специальности.

Рецензируемая учебная программа содержит следующие элементы: цели и задачи дисциплины, требования к уровню освоения содержания учебной дисциплины, соотнесенные с перечнем планируемых результатов обучения, межпредметные связи дисциплины, содержание учебного материала, учебно-методическую карту дисциплины, структурированную по темам и разделам с указанием отведенного на них количества академических часов и видов учебных занятий, список основной и дополнительной литературы, перечень вопросов для проведения зачета, описание содержания самостоятельной работы студентов и организации контроля качества усвоения знаний, характеристику инновационных подходов к преподаванию учебной дисциплины.

Тематический план учебной дисциплины имеет оптимальное распределение часов по разделам и темам в соответствии с учебным планом. Каждый раздел программы отражает тематику и вопросы, позволяющие в полном объеме изучить необходимый материал. Для выработки практических навыков предусмотрено необходимое количество лабораторных работ по темам дисциплины.

Предлагаемая к использованию основная и дополнительная литература позволит эффективно организовать не только изучение предлагаемых тем на занятиях, но и самостоятельную работу студентов. Подходы к организации контроля качества усвоения знаний обеспечивают объективность и достоверность результатов при проведении текущего контроля и промежуточной аттестации.

Представленная на рецензию учебная программа учреждения образования по учебной дисциплине «Криптографические методы защиты информации» для специальности 6-05-0533-12 «Кибербезопасность».

Рецензент:

Технический директор ООО «ТриИнком»,
к.т.н., доцент К.Я. Раханов