Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный
университет имени
Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«13» 12 2025 г.
Регистрационный №УД-482/25/уч

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И ДАННЫХ

Учебная программа учреждения образования
по учебной дисциплине для специальностей общего
и специального высшего образования

2025 г.

Учебная программа составлена на основе учебных планов учреждения образования по специальностям общего и специального высшего образования для дневной формы получения образования.

СОСТАВИТЕЛЬ:

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

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 11 от 21 11 2025 г.).

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 3 от 15 12 2025 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Интенсивное внедрение информационных технологий во все области деятельности человека позволяет обеспечить оперативный обмен сведениями между службами, отделами предприятия и организациями в целом за счет оптимизации информационных потоков, что позволяет ускорить и сделать более качественным процесс их взаимодействия. Сведения, которыми обмениваются такие партнеры, как правило, носят конфиденциальный характер и относятся к категориям служебной или государственной тайны, что требует подготовки современных специалистов, обладающих не только специальными знаниями по их профилю обучения, но и владением основами защиты информации.

Учебная дисциплина «Методы и средства обеспечения безопасности информационных систем и данных» ориентирована на обучение студентов гуманитарных, экономических и технических специальностей базовым знаниям, умениям и навыкам в области защиты информации. Изучаемые темы по модулю представляются на основе современной нормативной регулятивной базы и национального законодательства.

Целью изучения дисциплины «Методы и средства обеспечения безопасности информационных систем и данных» является формирование у студентов базовых знаний в области информационной безопасности и вопросов обеспечения защиты информации в условиях различных по виду, происхождению и характеру возникновения угроз.

При изучении дисциплины «Методы и средства обеспечения безопасности информационных систем и данных» требуется разрешить основные **задачи:**

– сформировать у студентов понимание базовых понятий, связанных с процессом обеспечения информационной безопасности;

– сформировать системное понимание проблем безопасности и путей их решения;

– изучить методы и средства защиты информации;

– получить знания о принципах организации и построения комплексных систем защиты информации.

При изучении дисциплины «Методы и средства обеспечения безопасности информационных систем и данных» у студентов специальностей должна сформироваться ***специализированная компетенция:***

Осуществлять поиск, критический анализ информации, применять системный подход для решения поставленных задач в самостоятельной деятельности, вырабатывать стратегию действий, генерировать и реализовывать инновационные идеи, осуществлять социальное взаимодействие и реализовывать свою роль в команде.

В результате изучения дисциплины «Методы и средства обеспечения безопасности информационных систем и данных» обучаемый должен:

знать:

– организационно-технические методы и технические средства защиты информации;

– основы криптографической защиты информации;

– особенности защиты информации в автоматизированных системах;

уметь:

– определять возможные каналы утечки информации и обоснованно выбирать средства их блокирования;

– разрабатывать рекомендации по защите объектов различного типа от несанкционированного доступа;

владеть:

– методами построения надежных криптосистем и функций хеширования;

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

Связи с другими учебными дисциплинами.

Основой для изучения учебной дисциплины «Методы и средства обеспечения безопасности информационных систем и данных» являются дисциплины «Математика»,

«Информатика», «Информационные технологии», изучаемые при получении общего базового и общего среднего образования.

Форма получения высшего образования - дневная

В соответствии с учебными планами специальностей общего и специального высшего образования на изучение учебной дисциплины отводится:

Курс (курсы)	3
Семестр	6
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	62
Лекции, часов	30
Практические занятия, часов	32
Самостоятельная работа по дисциплине, часов	46
Форма промежуточной аттестации по дисциплине	экзамен
Трудоёмкость дисциплины, з.е.	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ДАННЫХ

Тема 1.1. Информация как объект защиты.

Понятие об информации как объекте защиты. Уровни представления информации. Виды и формы представления информации. Информационные ресурсы. Компьютерная система как объект защиты. Конфиденциальность, целостность и доступность.

Тема 1.2. Угрозы информационной безопасности.

Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Уровни и направления обеспечения информационной безопасности.

Раздел 2. ЗАЩИТА ОТ УГРОЗЫ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ

Тема 2.1. Принципы криптографической защиты информации.

Криптография как наука. Основные термины и определения. Криптосистемы. Требования к криптосистемам. Типы атак. Сложность атак.

Тема 2.2. Классические криптосистемы.

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

Тема 2.3. Алгоритмы генерации псевдослучайной последовательности.

Псевдослучайная последовательность. Классификация алгоритмов генерации. Конгруэнтные генераторы. Рекурренты в конечном поле. Методы улучшения элементарных псевдослучайных последовательностей.

Тема 2.4. Шифры с гаммированием.

Шифрование методом гаммирования. Гамма шифра. Регистры сдвига с линейной обратной связью. Потоковые шифры.

Тема 2.5. Блочные симметричные криптосистемы.

Блочно-итерационные криптосистемы. Криптосистемы Фейстеля. Криптосистема DES. Криптосистема ГОСТ 28147-89. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью.

Тема 2.6. Асимметричные криптосистемы.

Общие принципы построения современных асимметричных криптосистем. Протокол Диффи-Хеллмана. Однонаправленные функции. Криптосистема RSA. Криптосистема Рабина. Криптосистема Эль-Гамаля.

Раздел 3. ЗАЩИТА ОТ УГРОЗЫ НАРУШЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Тема 3.1. Функции хеширования.

Однонаправленные хеш-функции. Блочно-итерационные функции хеширования. Функция хеширования СТБ 34.101.31. Атака «дней рождения».

Тема 3.2. Электронная цифровая подпись.

Обобщенная модель ЭЦП. Особенности применения асимметричных и симметричных криптосистем для ЭЦП. ЭЦП RSA. ЭЦП Эль-Гамаля. ЭЦП Шнорра. Система ЭЦП СТБ 1176.2. Защита целостности информации при хранении, обработке и транспортировке.

Раздел 4. ЗАЩИТА ОТ УГРОЗЫ ОТКАЗА ДОСТУПА

Тема 4.1. Идентификация и аутентификация.

Определение понятий идентификация, аутентификация и авторизация. Разновидности протоколов аутентификации. Протоколы аутентификации, основанные на использовании одноразового пароля. Протоколы аутентификации, основанные на пароле пользователя. Протоколы аутентификации, основанные на использовании симметричного алгоритма

шифрования, цифровой подписи и кода аутентификации сообщений. Протоколы идентификации с нулевым разглашением. Биометрическая идентификация и аутентификация пользователей.

Тема 4.2. Управление ключами в криптографических системах и протоколах.

Определение криптографического ключа и ключевой системы, основные функции по управлению ключами. Типы ключей в зависимости от практического использования. Способы распределения ключей.

Раздел 5. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Тема 5.1. Безопасность данных в компьютерных системах.

Политика безопасности компьютерных сетей. Угрозы безопасности информации в компьютерных системах. Компьютерные вирусы и методы борьбы с ними. Межсетевое экранирование. Защита сетевого трафика. Виртуальные защищенные сети. Методы мониторинга состояния сети.

Тема 5.2. Безопасность распределенных приложений.

Безопасность баз данных. Безопасность электронной почты. Безопасность платежных систем и аукционов. Безопасность социальных сетей. Облачная безопасность.

Учебно-методическая карта учебной дисциплины
«Методы и средства обеспечения безопасности информационных систем и данных»

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	**Безопасность информационных систем и данных.**	**4**		**2**			
Тема 1.1	***Информация как объект защиты.*** Понятие об информации как объекте защиты. Уровни представления информации. Виды и формы представления информации. Информационные ресурсы. Компьютерная система как объект защиты. Конфиденциальность, целостность и доступность.	2				Осн. лит.: [1], [2], [6]. Доп. лит.: [1].	Блиц-опрос
Тема 1.2	***Угрозы информационной безопасности.*** Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Уровни и направления обеспечения информационной безопасности.	2				Осн. лит.: [1], [2], [6]. Доп. лит.: [1].	Блиц-опрос
	Практическая работа №1. Основы теории чисел и их использование в криптографии.			2		Методические указания	Защита отчета по практической работе
Раздел 2	**Защита от угрозы нарушения конфиденциальности.**	**12**		**18**			
Тема 2.1	***Принципы криптографической защиты информации.*** Криптография как наука. Основные термины и определения. Криптосистемы. Требования к криптосистемам. Типы атак. Сложность атак.	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	Блиц-опрос

1	2	3	4	5	6	7	8
Тема 2.2	***Классические криптосистемы.*** Шифры перестановки. Шифры простой замены. Аффинный шифр. Шифры многоалфавитной замены. Шифр Хилла. Шифр Виженера.	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	Блиц-опрос
	Практическая работа №2. Защита данных с использованием криптоалгоритмов перестановки.			2		Методические указания	Защита отчета по практической работе
	Практическая работа №3. Защита данных с использованием криптоалгоритмов простой замены.			2		Методические указания	Защита отчета по практической работе
	Практическая работа №4. Защита данных с использованием криптоалгоритмов многоалфавитной замены.			2		Методические указания	Защита отчета по практической работе
Тема 2.3	***Алгоритмы генерации псевдослучайной последовательности.*** Псевдослучайная последовательность. Классификация алгоритмов генерации. Конгруэнтные генераторы. Рекурренты в конечном поле. Методы улучшения элементарных псевдослучайных последовательностей.	2				Осн. лит.: [2], [5], [6]. Доп. лит.: [2].	Блиц-опрос
	Практическая работа №5. Анализ генераторов псевдослучайной последовательности.			2		Методические указания	Защита отчета по практической работе
Тема 2.4	***Шифры с гаммированием.*** Шифрование методом гаммирования. Гамма шифра. Регистры сдвига с линейной обратной связью. Потоковые шифры.	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	Блиц-опрос
	Практическая работа №6. Защита данных с использованием криптоалгоритмов с гаммированием.			2		Методические указания	Защита отчета по практической работе
Тема 2.5	***Блочные симметричные криптосистемы.*** Блочно-итерационные криптосистемы. Криптосистемы Фейстеля. Криптосистема DES. Криптосистема ГОСТ 28147-89. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью.	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	Блиц-опрос
	Практическая работа №7. Защита данных с использованием блочных симметричных криптосистем.			2		Методические указания	Защита отчета по практической работе

1	2	3	4	5	6	7	8
	Практическая работа №7. Защита данных с использованием блочных симметричных криптосистем.			2		Методические указания	Защита отчета по практической работе
Тема 2.6	***Асимметричные криптосистемы.*** Общие принципы построения современных асимметричных криптосистем. Протокол Диффи-Хеллмана. Однонаправленные функции. Криптосистема RSA. Криптосистема Рабина. Криптосистема Эль-Гамаля.	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	Защита отчета по практической работе
	Практическая работа №8. Защита данных с использованием асимметричных криптосистем.			2		Методические указания	Блиц-опрос
	Практическая работа №8. Защита данных с использованием асимметричных криптосистем.			2			
Раздел 3	**Защита от угрозы нарушения целостности информации.**	**4**		**4**			
Тема 3.1	***Функции хеширования.*** Однонаправленные хеш-функции. Блочно-итерационные функции хеширования. Функция хеширования СТБ 34.101.31. Атака «дней рождения».	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	Блиц-опрос
Тема 3.2	***Электронная цифровая подпись.*** Обобщенная модель ЭЦП. Особенности применения асимметричных и симметричных криптосистем для ЭЦП. ЭЦП RSA. ЭЦП Эль-Гамаля. ЭЦП Шнорра. Система ЭЦП СТБ 1176.2. Защита целостности информации при хранении, обработке и транспортировке.	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	Блиц-опрос
	Практическая работа №9. Обеспечение подлинности и целостности электронных документов с использованием ЭЦП.			2		Методические указания	Защита отчета по практической работе
	Практическая работа №9. Обеспечение подлинности и целостности электронных документов с использованием ЭЦП.			2			
Раздел 4	**Защита от угрозы отказа доступа.**	**6**		**6**			

1	2	3	4	5	6	7	8
Тема 4.1	***Идентификация и аутентификация.*** Определение понятий идентификация, аутентификация и авторизация. Разновидности протоколов аутентификации. Протоколы аутентификации, основанные на использовании одноразового пароля. Протоколы аутентификации, основанные на пароле пользователя.	2				Осн. лит.: [2], [3], [6]. Доп. лит.: [2].	Блиц-опрос
	Протоколы аутентификации, основанные на использовании симметричного алгоритма шифрования, цифровой подписи и кода аутентификации сообщений. Протоколы идентификации с нулевым разглашением. Биометрическая идентификация и аутентификация пользователей.	2					
	Практическая работа №10. Разработка схемы простого пароля.			2		Методические указания	Защита отчета по практической работе
	Практическая работа №11. Разработка схемы динамического пароля.			2		Методические указания	Защита отчета по практической работе
Тема 4.2	***Управление ключами в криптографических системах и протоколах.*** Определение криптографического ключа и ключевой системы, основные функции по управлению ключами. Типы ключей в зависимости от практического использования. Способы распределения ключей.	2				Осн. лит.: [2], [3], [6]. Доп. лит.: [2].	Блиц-опрос
	Практическая работа №12. Защита данных с использованием протокола Диффи-Хеллмана.			2		Методические указания	Защита отчета по практической работе
Раздел 5	**Безопасность компьютерных систем.**	**4**		**2**			
Тема 5.1	***Безопасность данных в компьютерных системах.*** Политика безопасности компьютерных сетей. Угрозы безопасности информации в компьютерных системах. Компьютерные вирусы и методы борьбы с ними. Межсетевое экранирование. Защита сетевого трафика. Виртуальные защищенные сети. Методы мониторинга состояния сети.	2				Осн. лит.: [1], [4]. Доп. лит.: [1].	Блиц-опрос
Тема 5.2	***Безопасность распределенных приложений.*** Безопасность баз данных. Безопасность электронной почты. Безопасность платежных систем и аукционов. Безопасность социальных сетей. Облачная безопасность.	2				Осн. лит.: [1], [4]. Доп. лит.: [1].	Блиц-опрос

1	2	3	4	5	6	7	8
	Практическая работа №13. Защита компьютерных систем.			2		Методические указания	Защита отчета по практической работе
	Всего (62 часа)	**30**		**32**			

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. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург : Лань, 2025. — 280 с. – ISBN 978-5-507-50467-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 30.09.2025). – Режим доступа: для авториз. пользователей.

2. 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.

3. 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).

4. Раханов, К. Я. Обеспечение конфиденциальности информации в сети Интернет: пособие / К. Я. Раханов, Н. А. Раханова. – Новополоцк : Полоц. гос. ун-т, 2021. – 192 с.

5. 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»).

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

Нормативные документы:

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Взамен: ГОСТ Р 50922-96; введ. 2008-02-01. – М.: Стандартинформ, 2007. – 12 с.

2. СТБ 34.101.8-2006 Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования: введен 01.07.2006.

3. СТБ 34.101.9-2004 Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы: введен 01.09.2004.

Буркова Е.В.

4. СТБ 34.101.10-2004 Информационные технологии. Средства защиты информации от несанкционированного доступа в автоматизированных системах. Общие требования: введен 01.09.2004.

5. СТБ 34.101.12-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества: введен 01.10.2007.

6. СТБ 34.101.31-2011 Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности: введен 01.07.2011.

48. Протоколы аутентификации, основанные на использовании цифровой подписи.
49. Протоколы аутентификации, основанные на использовании кода аутентификации сообщений.
50. Протоколы идентификации с нулевым разглашением.
51. Биометрическая идентификация и аутентификация пользователей.
52. Определение криптографического ключа и ключевой системы, основные функции по управлению ключами.
53. Типы ключей в зависимости от практического использования.
54. Способы распределения ключей.
55. Политика безопасности компьютерных сетей.
56. Угрозы безопасности информации в компьютерных системах.
57. Компьютерные вирусы и методы борьбы с ними.
58. Межсетевое экранирование.
59. Защита сетевого трафика.
60. Виртуальные защищенные сети.
61. Методы мониторинга состояния сети.
62. Безопасность баз данных.
63. Безопасность электронной почты.
64. Безопасность платежных систем и аукционов.
65. Безопасность социальных сетей.
66. Облачная безопасность.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение 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 практических работ (предварительное знакомство с методическими указаниями, вариантом индивидуального задания по работе);

– решение индивидуальных задач при подготовке к практическим занятиям;

–подготовка к защите практических 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 экзамену.

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

– наличием и использованием в образовательном процессе СДО Moodle, доступной пользователям через Интернет в любое удобное для них время;

–наличием и полной доступностью электронных вариантов учебно-методических указаний по основным разделам дисциплины.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещённые в СДО Moodle для групповой работы и общения s: режим доступа **https://study.psu.by/course/edit.php?id=588**.

Содержание самостоятельной работы студентов (дневная форма получения высшего образования)

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	*Тема 2.2. Классические криптосистемы.* Шифры перестановки. Шифры простой замены. Аффинный шифр. Шифры многоалфавитной замены. Шифр Хилла. Шифр Виженера. Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	1
	Тема 2.4. Шифры с гаммированием. Шифрование методом гаммирования. Гамма шифра. Регистры сдвига с линейной обратной связью. Потоковые шифры.цепной обработки. Режим гаммирования с обратной связью. Осн. лит.: [2], [5], [6]. Доп. лит.: [2].	1
	Тема 2.5. Блочные симметричные криптосистемы. Криптосистемы Фейстеля. Криптосистема DES. Криптосистема ГОСТ 28147-89. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью. Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	1
	Тема 2.6. Асимметричные криптосистемы. Протокол Диффи-Хеллмана. Однонаправленные функции. Криптосистема RSA. Криптосистема Рабина. Криптосистема Эль-Гамаля. Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	1
	Тема 3.1. Функции хеширования. Однонаправленные хеш-функции. Блочно-итерационные функции хеширования. Функция хеширования СТБ 34.101.31. Атака «дней рождения». Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	1
	Тема 3.2. Электронная цифровая подпись. ЭЦП RSA. ЭЦП Эль-Гамаля. ЭЦП Шнорра. Система ЭЦП СТБ 1176.2. Защита целостности информации при хранении, обработке и транспортировке. Осн. лит.: [2], [3], [5]. Доп. лит.: [2].	1
	Тема 4.1. Идентификация и аутентификация. Протоколы аутентификации, основанные на использовании одноразового пароля. Протоколы аутентификации, основанные на пароле пользователя. Протоколы аутентификации, основанные на использовании симметричного алгоритма шифрования, цифровой подписи и кода аутентификации сообщений. Протоколы идентификации с нулевым разглашением. Осн. лит.: [2], [3], [6]. Доп. лит.: [2].	1
	Тема 4.2. Управление ключами в криптографических системах и протоколах. Определение криптографического ключа и ключевой системы, основные функции по управлению ключами. Типы ключей в зависимости от практического использования. Способы распределения ключей. Осн. лит.: [2], [3], [6]. Доп. лит.: [2].	1

1	2	3
	Тема 5.1. Безопасность данных в компьютерных системах. Политика безопасности компьютерных сетей. Угрозы безопасности информации в компьютерных системах. Компьютерные вирусы и методы борьбы с ними. Межсетевое экранирование. Защита сетевого трафика. Виртуальные защищенные сети. Методы мониторинга состояния сети. Осн. лит.: [1], [4]. Доп. лит.: [1].	1
	Тема 5.2. Безопасность распределенных приложений. Безопасность баз данных. Безопасность электронной почты. Безопасность платежных систем и аукционов. Безопасность социальных сетей. Облачная безопасность. Осн. лит.: [1], [4]. Доп. лит.: [1].	1
Подготовка к защите отчетов по практическим работам	*Практическая работа №1.* Основы теории чисел и их использование в криптографии.	2
	Практическая работа №2. Защита данных с использованием криптоалгоритмов перестановки	2
	Практическая работа №3. Защита данных с использованием криптоалгоритмов простой замены.	2
	Практическая работа №4. Защита данных с использованием криптоалгоритмов многоалфавитной замены.	2
	Практическая работа №5. Анализ генераторов псевдослучайной последовательности.	2
	Практическая работа №6. Защита данных с использованием криптоалгоритмов с гаммированием..	2
	*Практическая работа №7.*Защита данных с использованием блочных симметричных криптосистем.	2
	Практическая работа №8. Защита данных с использованием асимметричных криптосистем.	2
	Практическая работа №9. Обеспечение подлинности и целостности электронных документов с использованием ЭЦП.	2
	*Практическая работа №10.*Разработка схемы простого пароля.	2
	*Практическая работа №11.*Разработка схемы динамического пароля.	2
	Практическая работа №12. Защита данных с использованием протокола Диффи-Хеллмана.	2
	Практическая работа №13. Защита компьютерных систем.	2
Подготовка к экзамену		10
		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 (письменные отчёты по практическим работам);

–устно-письменная форма (отчёты по практическим работам с их устной защитой).

Для оценивания самостоятельной и аудиторной работы студентов в рамках учебной дисциплины для контроля успеваемости используется накопительная система, которая предполагает суммирование отметок, выставляемых в электронный журнал за все виды работ в течение семестра, для определения среднеарифметических показателей успеваемости.

Практические работы предполагают выполнение и защиту. При выполнении практических работ выдаётся индивидуальное задание. Отчёт по практической 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:

$$\text{Т} = \frac{(\text{ПР}_1 + \cdots + \text{ПР}_{n2}) + (\text{УО}_1 + \cdots + \text{УО}_{n3})}{(n2 + n3)},$$

где $\text{ПР}_1, \ldots, \text{ПР}_{n2}$ – отметки, выставленные по результатам защит практических работ; $n2$ – количество работ; $\text{УО}_1, \ldots, \text{УО}_{n3}$ – 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 экзамена в шестом семестре.

Итоговая экзаменационная отметка по дисциплине рассчитывается по формуле:

$$\text{ИЭ} = k \cdot \text{Т} + (1 - k) \cdot O,$$

где k – весовой коэффициент текущего контроля; Т – результат текущего контроля за семестр; О – отметка, полученная студентом на экзамене за ответ по билету.

Весовой коэффициент принимается равным $k = 0.5$.

Результат итоговой экзаменационной отметки округляется до целого значения.

Информация о весовом коэффициенте доводится до студентов на первом занятии в семестре. Положительной является отметка не ниже 4 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.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Методы и средства обеспечения безопасности информационных систем и данных» 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 «Методы и средства обеспечения безопасности информационных систем и данных» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных занятиях, на которых студенты овладевают системой теоретических знаний в области защиты информации и информационной безопасности и формируют системное понимание проблем защиты информации и информационной безопасности и путей их решения, и практических занятий, на которых развиваются и формируются необходимые практические умения и навыки.

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 политехнический кругозор, использованием интерактивных методов обучения.

Во время проведения практических работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.