Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
4	3	108	15	30	15		48	0	З
Итого	3	108	15	30	15	12	48	0	

АННОТАЦИЯ

Целью освоения учебной дисциплины «Основы криптографической защиты информации» является формирование общих представлений о криптографических методах, лежащих в основе обеспечения информационной безопасности и средствах, а также основных криптографических протоколах.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Основы криптографической защиты информации» является получение знаний и выработка компетенций в области криптографической защиты информации в организациях.

В результате освоения дисциплины студент должен

знать:

основы криптографической защиты информации;

руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к криптографической защите информации организации;

основные понятия и требования криптографической защиты информации;

уметь:

организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам криптографической защиты информации;

выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации;

выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации;

владеть:

навыками определения криптографической стойкости шифрсистем;

навыками выбора, исследовать эффективность и разрабатывать технико-экономическое обоснование проектных решений средств и систем криптографической защиты информации с целью обеспечения требуемого уровня защищенности;

навыками обоснования выбора криптографических средств для защиты информации.

Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

строгость в суждениях,

творческое мышление,

организованность и работоспособность,

дисциплинированность,

самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Основы криптографической защиты информации» является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина «Основы криптографической защиты информации» относится к числу дисциплин вариативной части общенаучного цикла.

Учебная дисциплина является базой для изучения следующих учебных дисциплин и/или составных частей учебных дисциплин направления подготовки 10.04.01 «Информационная безопасность»: «Технологии обеспечения информационной безопасности объектов», «Технологии построения защищенных автоматизированных систем».

Для усвоения учебной дисциплины «Основы криптографической защиты информации» студенты должны знать следующие дисциплины: «Математический анализ»; «Линейная алгебра»; «Общая алгебра»; «Теория вероятностей и математическая статистика»; «Дискретная математика»; «Информатика»; «Теория информации»; «Основы информационной безопасности», «Технологии и методы программирования».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.030, 06.032, 06.033, 06.034	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности

			используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты

			информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
Проектирование систем обеспечения информационной безопасности (СОИБ)	Средства и технологии обеспечения безопасности значимых объектов критической информационной	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы

конкретных объектов на стадиях разработки, эксплуатации и модернизации	инфраструктуры	ИБ иди информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа. ; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче

			информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее. ; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного

			доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	З-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические

			документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить

			экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные

			(программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.
организационно-управленческий			
Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	Контроль защищенности информации на объектах информатизации	ПК-8 [1] - Способен использовать навыки составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области ИБ или в области информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.033, 06.034	З-ПК-8[1] - Знать: профессиональная и криптографическая терминология в области безопасности информации; эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения. организационно-распорядительная документация по защите информации на объекте информатизации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); технические каналы

			утечки акустической речевой информации; методы защиты информации от утечки по техническим каналам; способы защиты акустической речевой информации от утечки по техническим каналам. ; У-ПК-8[1] - Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять перечень информации (сведений)ограниченного доступа, подлежащих защите в организации; определять условия расположения объектов информатизации относительно границ контролируемой зоны; разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации; разрабатывать разрешительную систему доступа к информационным ресурсам, программным

			и техническим средствам автоматизированных (информационных) систем организации. ; В-ПК-8[1] - Владеть: основами применения средств схемотехнического проектирования и современной измерительной аппаратуры; основами оптимизации работ электронных схем с учетом требований по защите информации; основами организации проведения научных исследований по вопросам технической защиты информации, выполняемых в организации.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	4 Семестр						
1	Математические аспекты криптографии	1-8	8/16/8		25	КИ-8	З-ПК-1, У-ПК-1, З-ПК-2, У-ПК-2, З-ПК-4, У-ПК-4, З-ПК-8, У-ПК-8

2	Системные и прикладные аспекты криптографии	9-15	7/14/7		25	КИ-15	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-8, У-ПК-8, В-ПК-8
	Итого за 4 Семестр		15/30/15		50		
	Контрольные мероприятия за 4 Семестр				50	ЗО	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-8, У-ПК-8, В-ПК-8

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
ЗО	Зачет с оценкой
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	4 Семестр	15	30	15
1-8	**Математические аспекты криптографии**	8	16	8
1 - 2	**Математические основы криптографии** Ведение в дисциплину. Делимость чисел. Признаки делимости. Простые и составные числа. Основная теорема арифметики. Наибольший общий делитель (НОД). Взаимно простые числа. Алгоритм Евклида нахождения НОД. Расширенный алгоритм Евклида. Функция Эйлера. Элементы теории множеств. Бинарные операции. Группы, кольца, поля. Отношение сравнимости. Свойства сравнений. Модулярная арифметика. Классы. Полная и приведенная системы вычетов.	Всего аудиторных часов 2 Онлайн 0	4 0	2 0
3 - 4	**Математические основы криптографии** Математические основы криптографии. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю. Сравнения первой степени. Линейные диофантовые уравнения. Китайская теорема об остатках. Проверка чисел на простоту. Алгоритм генерации простых чисел. Метод пробных делений. Решето Эратосфена. Алгоритм факторизации. Факторизация Ферма. Метод Полларда. Алгоритмы дискретного логарифмирования. Метод Полларда. Арифметические операции над большими числами. Эллиптические кривые.	Всего аудиторных часов 2 Онлайн 0	4 0	2 0
5 - 6	**Введение в криптографическую защиту информации** Открытые сообщения и их характеристики. k-граммная модель открытого текста. Критерии распознавания открытого текста. Основные задачи криптографии. Симметричное и ассиметричное шифрование. Классификация шифров. Модели шифров. Основные требования к шифрам. Криптографические протоколы.	Всего аудиторных часов 2 Онлайн 0	4 0	2 0
7 - 8	**Введение в криптографическую защиту информации** Кодирование, сжатие и шифрование информации. Символьное и смысловое кодирование информации. Представление информации в двоичном коде. Таблица ASCII. Сжатие информации. Шифры перестановки. Традиционные перестановки. Разновидности шифров перестановки. Поточные шифры замены. Применение генераторов псевдослучайных чисел в криптографии.	Всего аудиторных часов 2 Онлайн 0	4 0	2 0

	Методы получения псевдослучайных последовательностей.			
9-15	**Системные и прикладные аспекты криптографии**	7	14	7
9 - 10	**Системы шифрования** Симметричные системы шифрования. Структурная схема симметричных криптографических систем. Принципы построения криптографических алгоритмов. Отечественные и зарубежные криптоалгоритмы. Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хеллмана. Управление ключами. Протокол Kerberos. Ассиметричные системы шифрования. Системы шифрования открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Отечественные и зарубежные стандарты асимметричного шифрования. Системы шифрования RSA и Эль-Гамаля. Криптосистемы на основе эллиптических кривых. Безопасность асимметричных систем шифрования.	Всего аудиторных часов		
		2	4	2
		Онлайн		
		0	0	0
11 - 12	**Криптография и информационная безопасность. Применение криптографии.** Направления обеспечения информационной безопасности в Российской Федерации и за рубежом. Криптоанализ. Основные методы криптоанализа. Криптографические атаки и стойкость шифров. Абсолютно стойкие криптосистемы. Принцип Керкгоффса. Перспективные направления криптоанализа. Хеш-функции. Аутентификация. Электронная подпись. Защита информации в сетях передачи данных. Электронные аукционы.	Всего аудиторных часов		
		2	4	2
		Онлайн		
		0	0	0
13 - 14	**Модели инфраструктуры открытых ключей** Переход от бумажного к электронному документообороту. Инфраструктуры открытых ключей. Модели инфраструктуры открытых ключей. Североамериканская, западноевропейская и российская модели инфраструктуры открытых ключей. Криптографические методы защиты экономической информации. Новая «виртуальная социально-экономическая среда», «Кибер уязвимость». Системы электронной коммерции в сети Интернет. Характеристика IOTP-протоколов и PAPI-интерфейса.	Всего аудиторных часов		
		2	4	2
		Онлайн		
		0	0	0
15	**Компьютеризация шифрования** Аппаратное и программное шифрование. Стандартизация программно-аппаратных криптографических систем и средств. Современные программно-аппаратные криптографические средства. Проблемы и направления развития криптографии. Проблемы ограничения скорости шифрования. Проблемы теории ассиметричных алгоритмов. Квантовая криптография. Перспективы развития криптографии.	Всего аудиторных часов		
		1	2	1
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозна	**Полное наименование**

чение	
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	4 Семестр
1 - 2	**Лабораторная работа №1** Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации.
3 - 4	**Лабораторная работа №2** Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей
5 - 6	**Лабораторная работа №3** Использование стандарта симметричного шифрования AES RIJNDAEL
7 - 8	**Лабораторная работа №4** Генерация простых чисел, используемых в асимметричных системах шифрования.
9 - 10	**Лабораторная работа №5** Электронная цифровая подпись.
11 - 12	**Лабораторная работа №6** Шифр Плейфера.
13 - 14	**Лабораторная работа №7** Сеть Фейстеля.
15	**Лабораторная работа №8** Защита электронных документов с использованием цифровых водяных знаков.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач.

При реализации программы учебной дисциплины используются различные образовательные технологии – во время аудиторных занятий занятия проводятся в форме лекций и практических занятий.

Самостоятельная работа студентов подразумевает под собой проработку лекционного материала и выполнения домашнего задания в форме решения поставленных задач. Для контроля усвоения студентом разделов данного дисциплины используются домашние задания.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-1	З-ПК-1	ЗО, КИ-8, КИ-15
	У-ПК-1	ЗО, КИ-8, КИ-15
	В-ПК-1	ЗО, КИ-15
ПК-2	З-ПК-2	ЗО, КИ-8, КИ-15
	У-ПК-2	ЗО, КИ-8, КИ-15
	В-ПК-2	ЗО, КИ-15
ПК-4	З-ПК-4	ЗО, КИ-8, КИ-15
	У-ПК-4	ЗО, КИ-8, КИ-15
	В-ПК-4	ЗО, КИ-15
ПК-8	З-ПК-8	ЗО, КИ-8, КИ-15
	У-ПК-8	ЗО, КИ-8, КИ-15
	В-ПК-8	ЗО, КИ-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская
75-84		C	
70-74		D	

			существенных неточностей в ответе на вопрос.
65-69	3 – «*удовлетворительно*»	E	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64			
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Ф 76 Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов, Москва: Юрайт, 2022

2. ЭИ Ф 76 Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов, Москва: Юрайт, 2022

3. 0 О-75 Основы криптографии : Учеб. пособие для вузов, А. П. Алферов [et al.], Москва: Гелиос АРВ, 2002

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 0 Ф76 Методы дискретной математики в криптологии : учебное пособие для вузов, В. М. Фомичёв, Москва: Диалог-МИФИ, 2010

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. «Эволюция криптографии» (https://youtu.be/M9W4QpqQ5Ps)

2. «История криптографии» (https://youtu.be/c2gXHMQbzkM)

3. «Математические основы криптографии // Кольца»
(https://www.youtube.com/watch?v=DmeyD2vSSwI)

4. «Асимметричное шифрование» (https://www.youtube.com/watch?v=sGFbM-X6W_4)

5. «Алгоритм шифрования RSA» (https://www.youtube.com/watch?v=vooHjWxmcIE)

6. «Что такое хэш-функция» (https://www.youtube.com/watch?v=Bul0XYMa8Jg)

7. «Шифровальная машина Энигма» (https://www.youtube.com/watch?v=WBxwkMUxLcg)

8. «Русские шифровальные «Энигмы» (https://www.youtube.com/watch?v=Qnn6Th30qt8)

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы –Обеспечение безопасности значимых объектов критической информационной инфраструктуры, место курса в различных областях науки и техники. В том числе в области аттестации объектов информатизации по требованиям безопасности информации; в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области криптографической защиты информации, организационно-распорядительные, нормативные и информационные документы ФСБ России, ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющихся математической основой криптографии и криптографической защиты информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке практических навыков использования математических методов и программных средств криптографической защиты информации. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях и лабораторных работах.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области аттестации объектов информатизации по требованиям безопасности информации; в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области криптографической защиты информации, организационно-распорядительные, нормативные и информационные документы ФСБ России, ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющихся математической основой криптографии и криптографической защиты информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке практических навыков использования математических методов и программных средств криптографической защиты информации. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля

студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях и лабораторных работах.

1. Чтение лекций.

Первая лекция должна быть введением к дисциплине (разделу дисциплины, читаемому в начинающемся семестре). Она должна содержать общий обзор содержания дисциплины. В ней следует отметить методические инновации в решении задач, рассматриваемых в дисциплине, дать перечень рекомендованной литературы и вновь появившихся литературных источников, обратив внимание студентов на обязательную и дополнительную литературу.

Изложению текущего лекционного материала должна предшествовать вводная часть, содержащая краткий перечень вопросов, рассмотренных на предыдущих лекциях. На этом этапе полезно задать несколько вопросов аудитории, осуществить выборочный контроль знания студентов.

При изложении лекционного материала следует поощрять вопросы непосредственно в процессе изложения, внимательно относясь к вопросам студентов и при необходимости давая дополнительные, более подробные пояснения.

При чтении лекций преимущественное внимания следует уделять качественным вопросам, опуская простые математические выкладки, либо рекомендуя выполнить их самим студентам, либо отсылая студентов к литературным источникам и методическим пособиям.

В процессе лекционного курса необходимо возможно чаще возвращаться к основным вопросам дисциплины, проводя выборочный экспресс-контроль знаний студентов.

Принятая преподавателем система обозначений должна чётко разъясняться в процессе её введения и использоваться в конспектах лекций.

В лекциях, предшествующих практическим занятиям, следует кратко излагать содержание и основные задачи практического занятия, дать рекомендации студентам для подготовки к нему.

На последней лекции важно найти время для обзора основных положений,

рассмотренных в дисциплине, перечню и формулировке вопросов, выносимых на экзамен или зачёт.

2. Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Гавдан Григорий Петрович

Рецензент(ы):
Дураковский А.П.