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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ КРИПТОГРАФИИ

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**
1	2	72	16	0	0		56	0	З
Итого	2	72	16	0	0	0	56	0	

АННОТАЦИЯ

В курсе рассматриваются следующие темы:

- взаимосвязь стандартов, регламентирующих вопросы информационной безопасности,
- планирование и осуществление эффективных мероприятий, направленных на защиту информации на объекте информатизации,
- защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники,
- защита информации в государственных информационных системах,
- порядок разработки, производства, распространения и эксплуатации криптографических средств,
- защита персональных данных с использованием криптографических средств,
- особенности применения электронной подписи.

Подробно изучаются процессы разработки, производства, распространения и эксплуатации криптографических средств, а также порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных криптографических средств информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Особое внимание уделяется различным аспектам защиты персональных данных с использованием криптографических средств.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение основных стандартов и других нормативных документов, регулирующих вопросы защиты информации, разработки и применения криптографических средств.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные в результате освоения учебной дисциплины знания, умения, навыки используются в процессе дипломного проектирования.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-2 [1] – Способен управлять проектом на всех этапах его жизненного цикла	З-УК-2 [1] – Знать: этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами У-УК-2 [1] – Уметь: разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ; объяснить

	цели и сформулировать задачи, связанные с подготовкой и реализацией проекта; управлять проектом на всех этапах его жизненного цикла В-УК-2 [1] – Владеть: методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта

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			
разработка проектных решений по обеспечению безопасности данных с применением криптографических методов	информационные ресурсы	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы 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.

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
	1 Семестр						
1	Первый раздел	1-8	8/0/0	КИ-8 (25)	25	КИ-8	З-ПК-2, У-ПК-2, В-ПК-2, З-УК-2, У-УК-2, В-УК-2
2	Второй раздел	9-16	8/0/0	КИ-16 (25)	25	КИ-16	З-ПК-2, У-ПК-2,

							В-ПК-2, З-УК-2, У-УК-2, В-УК-2
	Итого за 1 Семестр		16/0/0		50		
	Контрольные мероприятия за 1 Семестр				50	З	З-ПК-2, У-ПК-2, В-ПК-2, З-УК-2, У-УК-2, В-УК-2

* – 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**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	1 Семестр	16	0	0
1-8	**Первый раздел**	8	0	0
1 - 2	**Основные стандарты РФ, регламентирующие вопросы защиты информации.** Стандартизация в области защиты информации. Краткая характеристика и взаимосвязь стандартов, регламентирующих вопросы информационной безопасности. Основные определения.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
3	**Факторы, воздействующие на защищаемую информацию.** Планирование и осуществление эффективных мероприятий, направленных на защиту информации на объекте информатизации. Выявление факторов, воздействующих на защищаемую информацию. Классификация и перечень факторов, воздействующих на безопасность защищаемой информации.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
4 - 5	**Защита средств вычислительной техники от несанкционированного доступа к информации.** Комплекс средств защиты информации. Защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники. Требования к защите средств вычислительной техники от несанкционированного доступа к информации. Требования к составу документации на средства вычислительной техники. Номенклатура показателей	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0

	защищенности средств вычислительной техники.			
6	**Архитектура защиты информации при взаимодействии открытых систем.** Услуги и механизмы защиты, которые могут быть обеспечены эталонной моделью, а также их реализация. Шифрование и электронная подпись как специальные механизмы защиты. Функции административного управления механизмами защиты.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
7	**Обеспечение безопасности критической инфраструктуры.** Принципы обеспечения безопасности критической информационной инфраструктуры. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы. Категорирование объекта критической информационной инфраструктуры. Система безопасности значимого объекта критической информационной инфраструктуры.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
8	**Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.** Требования к организации защиты информации, содержащейся в информационной системе. Разработка системы защиты информации информационной системы. Внедрение системы защиты информации информационной системы. Аттестация информационной системы и ввод ее в действие. Требования к мерам защиты информации, содержащейся в информационной системе. Определение класса защищенности информационной системы	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
9-16	**Второй раздел**	8	0	0
9	**Лицензирование разработки и производства криптографических средств.** Порядок лицензирования разработки, производства криптографических средств и защищенных с их использованием информационных систем.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
10 - 11	**Разработка, производство, реализация и эксплуатация криптографических средств.** Порядок разработки криптографических средств. Выбор носителя ключевой информации. Тематические исследования криптографических средств. Порядок производства криптографических средств. Порядок распространения криптографических средств. Порядок эксплуатации криптографических средств.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
12 - 13	**Безопасность информации при ее хранении, обработке и передаче по каналам связи с использованием криптографических средств.** Порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных криптографических средств информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Орган криптографической защиты и его функции.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0

	Обязанности пользователей криптографических средств.			
14 - 15	**Обеспечение безопасности персональных данных с использованием криптографических средств.** Порядок обеспечения безопасности персональных данных при помощи криптографических средств с использованием средств автоматизации. Обязанности оператора персональных данных. Формирование модели угроз персональным данным. Структура модели нарушителя.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
16	**Особенности применения электронной подписи** Основные нормативные документы, регулирующие вопросы применения электронной подписи и их краткая характеристика. Принципы использования электронной подписи. Виды электронной подписи. Требования к средствам электронной подписи и средствам удостоверяющего центра. Придание юридической значимости электронному документу.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
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

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии (лекции, практические работы с компьютерными технологиями) сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, влючают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятиий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы.

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-2	З-ПК-2	З, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-16
	В-ПК-2	З, КИ-8, КИ-16
УК-2	З-УК-2	З, КИ-8, КИ-16
	У-УК-2	З, КИ-8, КИ-16
	В-УК-2	З, КИ-8, КИ-16

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 существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		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		E	
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. 004 М 21 Комментарии к Доктрине информационной безопасности Российской Федерации. : , Малюк А.А., Полянская О.Ю., Москва: Горячая линия -Телеком, 2018

2. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Малюк А.А., Москва: Горячая линия -Телеком, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

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

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций и семинарских занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время семинарских занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

При необходимости в конце лекции преподаватель оставляет время для того, чтобы студенты имели возможность задать вопросы по изучаемому материалу.

Лекции нацелены на освещение основополагающих положений теории алгоритмов и теории функций алгебры логики, наиболее трудных вопросов, как правило, связанных с доказательством необходимых утверждений и теорем, призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на

лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого семинара.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе лекций, аудиторных практических занятий и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции. В лекционном курсе главное место отводится общетеоретическим проблемам.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и

средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Епишкина Анна Васильевна, к.т.н.