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 № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ (НАУЧНО-ТЕХНИЧЕСКИЙ СЕМИНАР)

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	2-3	72-108	20	0	20		32-88	0	З
Итого	2-3	72-108	20	0	20	0	32-88	0	

Москва, 2020

АННОТАЦИЯ

На основе Доктрины информационной безопасности Российской Федерации изучаются проблемы формирования информационного общества и связанный с этим рост уязвимости информации в условиях развития современных информационных технологий, анализируются и классифицируются угрозы безопасности информации в критических системах информационной инфраструктуры, конкретизируются задачи систем ее обеспечения. Дается обзор методов, технических приемов и аппаратуры защиты информации. Основное внимание уделяется проблемам опознавания пользователя, криптографическим методам защиты информации, методам защиты от компьютерных вирусов, защите от утечки информации по техническим каналам, организационно-правовому обеспечению безопасности информации. Подчеркивается необходимость комплексного подхода к защите информации, важность методологических проблем организации и обеспечения функционирования комплексной системы защиты. Излагаются основы информационной культуры как важнейшего фактора обеспечения безопасного развития информационного общества.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение общих вопросов обеспечения безопасности информации в критических системах.

В курсе рассматриваются следующие темы:

- история и современные проблемы информационной безопасности,
- уязвимость информации,
- защита информации от несанкционированного доступа,
- криптографические методы защиты информации,
- программы-вирусы,
- защита информации от утечки по техническим каналам,
- организационно-правовое обеспечение защиты информации,
- гуманитарные проблемы информационной безопасности,
- реализация концепции комплексной защиты информации.

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

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**
научно- исследовательский			
выполнение научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных	методы обеспечения безопасности данных	ПК-4.2 [1] - Способен участвовать в выполнении научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных *Основание:* Профессиональный стандарт: 06.032	З-ПК-4.2[1] - Знать: методы обеспечения безопасности данных; У-ПК-4.2[1] - Уметь: применять методы обеспечения безопасности данных; В-ПК-4.2[1] - Владеть: навыками выполнения научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных
выполнение научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных	методы обеспечения безопасности данных	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.032	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные

			стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

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	Первый раздел	1-8			25	КИ-8	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-3,

							У-ПК-3, В-ПК-3
2	Второй раздел	9-15			25	КИ-15	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 4 Семестр		20/0/20		50		
	Контрольные мероприятия за 4 Семестр				50	З	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-3, У-ПК-3, В-ПК-3

* – 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.**
	4 Семестр	20	0	20
1-8	**Первый раздел**	0	7	

1	**Уязвимость информации и проблемы обеспечения информационной безопасности** Информационное общество и информационная безопасность. Терминология и предметная область. Доктрина информационной безопасности Российской Федерации. Стратегия развития информационного общества в России. Исторический очерк развития подходов к обеспечению информационной безопасности. Проблема комплексности защиты. Формирование политики безопасности критических систем информационной инфраструктуры. Определение угрозы и уязвимости информации. Классификация угроз. Вредительские программы. Системная классификация угроз. Количественная оценка угроз. Понятие информационного риска. Информационное общество и изменение пространства военно-силового противоборства. Информационное оружие и информационная война. Основные цели информационной войны. Объекты информационного противоборства. Субъекты информационного противоборства. Психологические ресурсы общества.	Всего аудиторных часов		
			7	
		Онлайн		
9-15	**Второй раздел**	0	13	
2	**Программно-аппаратные методы защиты информации** Защита информации от несанкционированного доступа. Принципы защиты от несанкционированного доступа. Монитор обращений. Правила разграничения доступа. Вербальная модель разграничения доступа. Модель Хартсона. Модель Лэмпсона, Грэхема, Деннинга. Модель Белла и Ла Падула. Проблемы опознавания пользователя. Аутентификация по принципу «пользователь знает». Аутентификация по принципу «пользователь имеет». Аутентификация по принципу «пользователь есть». Характеристики устройств аутентификации. Схемы разграничения доступа.	Всего аудиторных часов		
			7	
		Онлайн		
3	**Программно-аппаратные методы защиты информации** Программы-вирусы. История проблемы. Компьютерные вирусы как специальный класс программ, обладающих свойством саморепродукции. Фазы существования компьютерного вируса. Средства антивирусной защиты. Вирусное подавление как форма информационной войны. Технические каналы утечки информации. Определение и основные виды каналов и источников утечки. Контроль акустической информации. Контроль информации в каналах связи. Контроль информации, обрабатываемой средствами вычислительной техники. Способы предотвращения утечки информации по техническим каналам. Защита от утечки информации по акустическому каналу. Защита информации в каналах связи. Защита информации от утечки по каналу побочных электромагнитных излучений и наводок.	Всего аудиторных часов		
			6	
		Онлайн		

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

Основными образовательными технологиями в освоении дисциплин профессионального цикла являются традиционные технологии лекций и лабораторных работ. Интерактивные методики обеспечиваются решением индивидуальных задач студентами и коллективным обсуждением результатов и методов решения.

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-3	З-ПК-3	З, КИ-8, КИ-15
	У-ПК-3	З, КИ-8, КИ-15
	В-ПК-3	З, КИ-8, КИ-15
ПК-4.2	З-ПК-4.2	З, КИ-8, КИ-15
	У-ПК-4.2	З, КИ-8, КИ-15
	В-ПК-4.2	З, КИ-8, 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

<table>
<tr><td></td><td></td><td></td><td>усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">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.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>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.</td></tr>
</table>

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Москва: Горячая линия -Телеком, 2018

2. 004 М 21 Комментарии к Доктрине информационной безопасности Российской Федерации. : , Москва: Горячая линия -Телеком, 2018

3. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., 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

приложены

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

приложены

Автор(ы):

Когос Константин Григорьевич, к.т.н.