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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МОНИТОРИНГ, АНАЛИТИКА И ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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**
2	4	144	30	30	0		48	0	Э
Итого	4	144	30	30	0	0	48	0	

АННОТАЦИЯ

Цель - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования, оценки и обработки рисков информационной безопасности.

Задачи дисциплины:

• изучение основных положений, понятий и категорий теоретических основ управления рисками информационной безопасности;

• изучение предпосылок для управления информационными рисками;

• изучение основных требований по управлению рисками информационной безопасности;

• изучение состава системы управления информационными рисками;

• формирование умений оценки рисков информационной безопасности;

• формирование умений обработки рисков информационной безопасности;

• формирование навыков по оценке угроз безопасности информации в технологии оценки рисков;

• формирование навыков подбора инструментальных средств для управления рисками информационной безопасности.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования, оценки и обработки рисков информационной безопасности.

Задачи дисциплины:

• изучение основных положений, понятий и категорий теоретических основ управления рисками информационной безопасности;

• изучение предпосылок для управления информационными рисками;

• изучение основных требований по управлению рисками информационной безопасности;

• изучение состава системы управления информационными рисками;

• формирование умений оценки рисков информационной безопасности;

• формирование умений обработки рисков информационной безопасности;

• формирование навыков по оценке угроз безопасности информации в технологии оценки рисков;

• формирование навыков подбора инструментальных средств для управления рисками информационной безопасности.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

дисциплина специализации

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 методов обеспечения информационной безопасности	методы обеспечения информационной безопасности	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.
выполнение научно-исследовательских работ по развитию методов обеспечения информационной безопасности	методы обеспечения информационной безопасности	ПК-8.1 [1] - Способен проводить мониторинг и проверку эффективности системы управления информационной безопасностью, а также непрерывное улучшение системы управления информационной безопасностью, основанное на результатах объективных измерений *Основание:* Профессиональный стандарт: 06.032	З-ПК-8.1[1] - Знать: основные методы мониторинга и повышения защищенности информации ; У-ПК-8.1[1] - Уметь: применять методики мониторинга и повышения защищенности информации; В-ПК-8.1[1] - Владеть: практическими навыками мониторинга и повышения защищенности информации конкретных организаций, в том числе объектов критической инфраструктуры
организационно-управленческий			
организовать эффективную работу по защите информационных ресурсов организации	информационные ресурсы	ПК-7 [1] - Способен планировать и организовывать предпроектное исследование объектов обеспечения ИБ или объектов информационно-аналитических систем безопасности	З-ПК-7[1] - Знать: основные методы организационного обеспечения информационной безопасности иас; основные виды угроз безопасности операционных систем; защитные механизмы и средства обеспечения

		Основание: Профессиональный стандарт: 06.032	безопасности операционных систем. ; У-ПК-7[1] - Уметь: организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; определять методы управления доступом, типы доступа и правила разграничения доступа; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях. ; В-ПК-7[1] - Владеть: основами формирования комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в иас информации ограниченного доступа.

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
	2 Семестр						
1	Первый раздел	1-8	15/15/0		25	КИ-8	З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-7, У-ПК-7, В-ПК-7, З-ПК-8.1, У-ПК-8.1, В-ПК-8.1
2	Второй раздел	9-15	15/15/0		25	КИ-15	З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-7, У-ПК-7, В-ПК-7, З-ПК-8.1, У-ПК-8.1, В-ПК-8.1
	Итого за 2 Семестр		30/30/0		50		
	Контрольные мероприятия за 2				50	Э	В-ПК-3,

	Семестр						З-ПК-7, У-ПК-7, В-ПК-7, З-ПК-8.1, У-ПК-8.1, В-ПК-8.1, З-ПК-3, У-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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	2 Семестр	30	30	0
1-8	**Первый раздел**	15	15	0
	Введение в дисциплину Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке магистров. Особенности формирования терминологии науч-ной дисциплины. Взаимосвязь курса с другими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература	Всего аудиторных часов		
		3	3	0
		Онлайн		
		3	0	0
	Предпосылки для управления информационными рисками Современные информационные риски и их особенности. Кибертерроризм. Риски промышленных	Всего аудиторных часов		
		3	3	0
		Онлайн		
		3	0	0

	систем. Риски утечки информации. Риски электронных расчетов. Стандарты управ-ления рисками. Государственное регулирование. Оценка рисков как основа корпоративного управления.			
	Основные требования по управлению рисками информационной безопасности Стандарты в области управления рисками информационной безопасности. Понятие риска. Оценка риска. Количественное определение величины риска. Качественное определение величины риска. Информационная составляющая бизнес - рисков. Активы организации как ключевые факторы риска. Подходы к управлению рисками. Уровни зрелости бизнеса в от-ношении рисков. Анализ факторов риска. Методика оценки рисков приватности, включая персональные данные	Всего аудиторных часов 3 Онлайн 3	 3 0	 0 0
	Система управления информационными рисками Преимущества системного подхода к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками. Процессная модель управления рисками. Непрерывная деятельность по управлению рисками. Сопровождение и мониторинг механизмов безопасности. Анализ со стороны руководства. Пересмотр и переоценка риска. Взаимосвязь процессов аудита и управления рисками. Управление документами и записями. Корректирующие и превентив-ные меры. Коммуникация рисков. Аутсорсинг процессов управления рисками. Распределе-ние ответственности за управление рисками. Требования к риск-менеджеру. Требования к эксперту по оценке рисков.	Всего аудиторных часов 3 Онлайн 3	 3 0	 0 0
	Оценка рисков информационной безопасности Идентификация активов. Описание бизнеспроцессов. Идентификация требований безопасности. Реестр требований безопасности. Требования законодательства и нормативной базы. Контрактные обязательства. Требования бизнеса. Определение ценности активов. Критерии оценки ущерба. Таблица ценности активов. Особенности интервьюирования бизнес-пользователей. Определение приоритетов аварийного восстановления.	Всего аудиторных часов 3 Онлайн 3	 3 0	 0 0
9-15	**Второй раздел**	15	15	0
	Оценка угроз безопасности информации в технологии оценки рисков Анализ угроз и уязвимостей. Профиль и жизненный цикл угрозы. Описание угроз безопасности. Способы	Всего аудиторных часов 3 Онлайн 3	 3 0	 0 0

	классификации угроз. Уязвимости информационной безопасности. Идентификация организационных уязвимостей. Идентификация технических уязвимостей. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Пример оценки риска. Отчет об оценке рисков.			
	Обработка рисков информационной безопасности Процесс обработки рисков. Способы обработки риска. Принятие риска. Уменьшение риска. Передача риска. Избегание риска. Оценка возврата инвестиций в информационную безопасность. Принятие решения по обработке риска. План обработки рисков. Декларация о применимости механизмов контроля. Профили рисков информационной безопасности.	Всего аудиторных часов		
		4	4	0
		Онлайн		
		4	0	0
	Инструментальные средства для управления рисками Актуальность программного сопровождения процедуры оценки рисков. Выбор программного обеспечения для оценки рисков. Общие недостатки и ограничения коммерческих про-граммных продуктов. Обзор методов и инструментальных средств управления рисками: OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise.	Всего аудиторных часов		
		4	4	0
		Онлайн		
		4	0	0
	Внедрение системы прогнозирования и управления рисками информационной безопасности Особенности внедрения системы управления информационными рисками (СУИР). Документация. Начальные условия для внедрения СУИР. Организационная структура управления рисками. Обучение членов экспертной группы. Проведение полной оценки рисков по всем активам. Жизненный цикл управления рисками.	Всего аудиторных часов		
		4	4	0
		Онлайн		
		4	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 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, современные (компьютерные) 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-3	З-ПК-3	Э, КИ-8, КИ-15
	У-ПК-3	Э, КИ-8, КИ-15
	В-ПК-3	Э, КИ-8, КИ-15
ПК-7	З-ПК-7	Э, КИ-8, КИ-15
	У-ПК-7	Э, КИ-8, КИ-15
	В-ПК-7	Э, КИ-8, КИ-15
ПК-8.1	З-ПК-8.1	Э, КИ-8, КИ-15
	У-ПК-8.1	Э, КИ-8, КИ-15
	В-ПК-8.1	Э, 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 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
75-84		C	
70-74		D	

			излагает его, не допуская существенных неточностей в ответе на вопрос.
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:

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, лабораторных 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.