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 ФБИУКС

Протокол № 24/08

от 22.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки (специальность) [1] 38.03.05 Бизнес-информатика

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**
7	1	36	24	0	0		12	0	З
Итого	1	36	24	0	0	0	12	0	

АННОТАЦИЯ

Целями освоения учебной дисциплины «Информационная безопасность» являются усвоение студентами основных положений Доктрины информационной безопасности Российской Федерации, Стратегии развития информационного общества в России, представления о предметной области комплекса наук о безопасности, качественных и количественных методах описания жизненно важных интересов личности, общества и государства, множества угроз безопасности, получение студентами знаний общих вопросов обеспечения безопасности информации в автоматизированных системах, ознакомление с основными понятиями и терминологией в области защиты данных и программ в компьютерах и компьютерных сетях, основными проблемами обеспечения безопасности информации, методами их решения, современными научными направлениями, связанными с решением этих проблем, воспитание в будущих специалистах правового сознания и морально-этических качеств, отвечающих требованиям этики в сфере информационных технологий.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Информационная безопасность» являются усвоение студентами основных положений Доктрины информационной безопасности Российской Федерации, Стратегии развития информационного общества в России, представления о предметной области комплекса наук о безопасности, качественных и количественных методах описания жизненно важных интересов личности, общества и государства, множества угроз безопасности, получение студентами знаний общих вопросов обеспечения безопасности информации в автоматизированных системах, ознакомление с основными понятиями и терминологией в области защиты данных и программ в компьютерах и компьютерных сетях, основными проблемами обеспечения безопасности информации, методами их решения, современными научными направлениями, связанными с решением этих проблем, воспитание в будущих специалистах правового сознания и морально-этических качеств, отвечающих требованиям этики в сфере информационных технологий.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Для изучения дисциплины необходимы знания математических дисциплин и основ информатики и 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	**Объект или**	**Код и наименование**	**Код и наименование**

профессиональной деятельности (ЗПД)	**область знания**	**профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**индикатора достижения профессиональной компетенции**
организационно-управленческий			
Организация проектирования, разработки, внедрения, эксплуатации компонентов архитектуры предприятий, планированием и управление проектами в этой области	Архитектура предприятия (бизнес-архитектура, архитектура информации, архитектура приложений, инфраструктура)	ПК-4 [1] - способен проводить обследования деятельности и ИТ-инфраструктуры предприятий *Основание:* Профессиональный стандарт: 06.014	З-ПК-4[1] - Знать: Стандарты и методики управления ИТ-инфраструктурой Стандарты и методики управления процессами ИТ ; У-ПК-4[1] - Узнать: Управлять процессами, оценивать и контролировать качество процессов управления ИТ-инфраструктурой; В-ПК-4[1] - Владеть навыками: Организация процесса выявления потребностей в ИТ-инфраструктуре Организация формирования задач управления ИТ-инфраструктурой на основе выявленных потребностей и согласование этих задач с заинтересованными лицами Инициирование и планирование выполнения задач управления ИТ-инфраструктурой и согласование с заинтересованными лицами этих планов Контроль выполнения задач управления ИТ-инфраструктурой Анализ результатов выполнения задач управления ИТ-

			инфраструктурой и выполнение управленческих действий по результатам анализа
Организация проектирования, разработки, внедрения, эксплуатации компонентов архитектуры предприятий, планированием и управление проектами в этой области	Архитектура предприятия (бизнес-архитектура, архитектура информации, архитектура приложений, инфраструктура)	ПК-5 [1] - способен осуществлять организацию и управление проектами в области информационных технологий в соответствии с требованиями заказчика *Основание:* Профессиональный стандарт: 06.014	З-ПК-5[1] - Знать: Теория программного управления ; У-ПК-5[1] - Узнать: Планировать и управлять программами проектов; В-ПК-5[1] - Владеть навыками: Формирование заказа программы проектов по созданию, развитию, выводу на рынок и продаже продуктов Передача заказа в ответственные подразделения Координирование выполнения программы проектов Прием результатов отдельных этапов работ программы
технологический			
Организация защиты интеллектуальной собственности, результатов исследований и программных разработок как коммерческой тайны	Архитектура предприятия (бизнес-архитектура, архитектура информации, архитектура приложений, инфраструктура)	ПК-7 [1] - способен защищать права на интеллектуальную собственность и результаты исследований и программных разработок как коммерческой тайны *Основание:* Профессиональный стандарт: 06.016, 40.001	З-ПК-7[1] - Знать: Правовые основы интеллектуальной собственности (ИС) Основы инновационной экономики Основные положения нормативных документов в области налогообложения, бухгалтерского, налогового и бюджетного учета и распоряжения бюджетными средствами, а также основы гражданского законодательства, имеющие отношение к распоряжению

			правами на ИС, правовой охране и защите прав на ИС Тенденции развития российского и международного рынка ИС Виды лицензионных договоров Правовые и экономические основы договоров по распоряжению исключительными правами на ИС Методы анализа эффективности управления системой ИС; У-ПК-7[1] - Уметь: Формировать эффективную систему управления ИС, используя методы системного анализа и теории управления, знания правовых и экономических основ ИС; В-ПК-7[1] - Владеть навыками: Разработка стратегий ИС организации, в том числе заключения лицензионных договоров Участие в создании системы информационного обеспечения процессов управления ИС Проведение анализа экономической эффективности управления портфелем ИС

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих,	Использование воспитательного потенциала дисциплин

	формирование культуры информационной безопасности (В23)	профессионального модуля для формирование базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.

5. 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
	7 Семестр						
1	Первый раздел	1-8	16/0/0		25	КИ-8	З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-5, У-ПК-5, В-ПК-5, З-ПК-7, У-ПК-7, В-ПК-7
2	Второй раздел	9-12	8/0/0		25	КИ-12	З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-5, У-ПК-5, В-ПК-5, З-ПК-7, У-ПК-7, В-ПК-7
	Итого за 7 Семестр		24/0/0		50		
	Контрольные мероприятия за 7 Семестр				50	З	З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-5, У-ПК-5, В-ПК-5,

							З-ПК-7, У-ПК-7, В-ПК-7

* – 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.**
	7 Семестр	24	0	0
1-8	**Первый раздел**	16	0	0
1	**Тема 1. История и современные проблемы информационной безопасности** Концепция безопасности как общая системная концепция развития общества. Информатизация общества и информационная безопасность. Доктрина информационной безопасности Российской Федерации. Стратегия развития информационного общества в России. Виды информационных опасностей. Терминология и предметная область защиты информации как науки и сферы деятельности. Комплексная защита информации.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
2 - 3	**Тема 2. Уязвимость информации** Угрозы безопасности информации и их классификация. Случайные угрозы. Преднамеренные угрозы. Вредоносные программы. Системная классификация угроз безопасности информации. Основные подходы к защите информации (примитивный подход, полусистемный подход, системный подход). Основные идеи и подходы к определению показателей уязвимости информации. Пятирубежная и семирубежная модели безопасности. Понятие информационного оружия и информационной войны. Международные аспекты информационной безопасности.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
4 - 5	**Тема 3. Защита информации от несанкционированного доступа** Основные принципы защиты информации от несанкционированного доступа. Принцип обоснованности доступа. Принцип достаточной глубины контроля доступа. Принцип разграничения потоков информации. Принцип чистоты повторно используемых ресурсов. Принцип персональной ответственности. Принцип целостности средств защиты. Классические модели защиты информации. Модель Хартсона. Модель безопасности с	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0

	"полным перекрытием". Модель Лэмпсона-Грэхема-Деннинга. Многоуровневые модели. Построение монитора обращений. Основные способы аутентификации терминальных пользователей. Аутентификация по паролю или личному идентифицирующему номеру. Аутентификация с помощью карт идентификации. Системы опознавания пользователей по физиологическим признакам. Аутентификация терминального пользователя по отпечаткам пальцев и с использованием геометрии руки. Методы аутентификации с помощью автоматического анализа подписи. Средства верификации по голосу. Методы контроля доступа.			
6	**Тема 4. Криптографические методы защиты информации** Общие сведения о криптографических методах защиты. Основные методы шифрования: метод замены, метод перестановки, метод на основе алгебраических преобразований, метод гаммирования, комбинированные методы Криптографические алгоритмы и стандарты криптографической защиты. Ключевая система. Ключевая система с секретными ключами. Ключевая система с открытыми ключами. Распределение ключей шифрования. Централизованные и децентрализованные системы распределения ключей. Алгоритм электронной цифровой подписи.	Всего аудиторных часов 2 Онлайн 0	0 0	0 0
7	**Тема 5. Программы -вирусы и основы борьбы с ними** Определение программ-вирусов, их отличие от других вредоносных программ. Фазы существования вирусов (спячка, распространение в вычислительной системе, запуск, разрушение программ и данных). Антивирусные программы. Программы проверки целостности программного обеспечения. Программы контроля. Программы удаления вирусов. Копирование программ как метод защиты от вирусов. Применение программ-вирусов в качестве средства радиоэлектронной борьбы.	Всего аудиторных часов 2 Онлайн 0	0 0	0 0
8	**Тема 6. Защита информации от утечки по техническим каналам** Понятие технического канала утечки информации. Виды каналов. Акустические и виброакустические каналы. Телефонные каналы. Электронный контроль речи. Канал побочных электромагнитных излучений и наводок. Электромагнитное излучение аппаратуры (видеотерминалов, принтеров, накопителей на магнитных дисках, графопостроителей и каналов связи сетей ЭВМ) и меры защиты информации. Способы экранирования аппаратуры, изоляция линий передачи путем применения различных фильтров, устройств подавления сигнала, низкоимпедансного заземления, трансформаторов развязки и др.	Всего аудиторных часов 2 Онлайн 0	0 0	0 0
9-12	**Второй раздел**	8	0	0
9	**Тема 7. Организационно-правовое обеспечение безопасности информации**	Всего аудиторных часов 2	 0	 0

	Государственная система защиты информации, обрабатываемой техническими средствами. Состояние правового обеспечения информатизации в России. Опыт законодательного регулирования информатизации за рубежом. Концепция правового обеспечения в области информатизации. Основные законодательные акты Российской Федерации в области обеспечения информационной безопасности. Организация работ по обеспечению безопасности информации. Система стандартов и руководящих документов по обеспечению защиты информации на объектах информатизации	Онлайн		
		0	0	0
10	**Тема 8. Гуманитарные проблемы информационной безопасности** Сущность и классификация гуманитарных проблем информационной безопасности. Постановка гуманитарных проблем в Доктрине информационной безопасности Российской Федерации. Развитие информационной культуры как фактора обеспечения информационной безопасности. Информационно-психологическая безопасность. Проблемы борьбы с внутренним нарушителем.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
11 - 12	**Тема 9. Комплексная система защиты информации** Синтез структуры системы защиты информации. Подсистемы СЗИ. Подсистема управления доступом. Подсистема учета и регистрации. Криптографическая подсистема. Подсистема обеспечения целостности. Задачи системы защиты информации. Оборонительная, наступательная и упреждающая стратегия защиты. Концепция защиты. Формирование полного множества функций защиты. Формирование репрезентативного множества задач защиты. Средства и методы защиты. Обоснование методологии управления системой защиты.	Всего аудиторных часов		
		4	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

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Занятия проводятся в активной и интерактивной форме с применением мнформационных технологий и мультимедийного оборудования.

7. 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-4	З-ПК-4	З, КИ-8, КИ-12
	У-ПК-4	З, КИ-8, КИ-12
	В-ПК-4	З, КИ-8, КИ-12
ПК-5	З-ПК-5	З, КИ-8, КИ-12
	У-ПК-5	З, КИ-8, КИ-12
	В-ПК-5	З, КИ-8, КИ-12
ПК-7	З-ПК-7	З, КИ-8, КИ-12
	У-ПК-7	З, КИ-8, КИ-12
	В-ПК-7	З, КИ-8, КИ-12

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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>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.</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 –</td><td>F</td><td>Оценка «неудовлетворительно»</td></tr>
</table>

	«*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.

8. 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/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. 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.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечение 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 лабораторных работах.

Автор(ы):

Малюк Анатолий Александрович, к.т.н., профессор