

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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-2/1

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки
(специальность)

[1] 10.05.05 Безопасность информационных технологий
в правоохранительной сфере

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
8	3	108	30	15	15		48	0	3
Итого	3	108	30	15	15	15	48	0	

АННОТАЦИЯ

Формирование принципов построения защищенных компьютерных систем, в том числе критически важных (ядерная энергетика, оборона, космос) компьютерных систем.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины являются изучение принципов построения защищенных компьютерных систем, в том числе критически важных (ядерная энергетика, оборона, космос) компьютерных систем.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Для успешного освоения дисциплины Защита информации необходимы компетенции, формируемые в результате освоения следующих дисциплин:

ЭВМ и периферийные устройства

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 соответствии 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
проектно-технологический			
Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации; участие в проектировании систем, комплексов средств и технологий	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного	ПК-1 [1] - Способен формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации <i>Основание:</i> Профессиональный стандарт: 06.033	З-ПК-1[1] - знать основные действующие нормативные и методологические документы в области безопасности информации, основы обеспечения безопасности информации ; У-ПК-1[1] - уметь формировать рабочую

<p>обработки и защиты информации, в разработке технологической и эксплуатационной документации; адаптация к защищаемым объектам современных информационных технологий и методов обеспечения безопасности информации на основе отечественных и международных стандартов</p>	<p>уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового</p>		<p>техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации; В-ПК-1[1] - владеть навыками формирования рабочей технической документации в области безопасности информации для целей профессиональной деятельности</p>
--	---	--	--

	мониторинга в субъектах первичного финансового мониторинга.		
эксплуатационный			
Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонент технических систем обеспечения безопасности информации; участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации; администрирование подсистем обеспечения информационной безопасности на объекте.	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической	ПК-3 [1] - Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-3[1] - знать основные нормативно-правовые акты и методические документы по обеспечению защиты информации и организационные основы контроля обеспечения защиты информации, в том числе сведений, составляющих государственную тайну, а также методики анализа эффективности систем защиты информации ; У-ПК-3[1] - уметь организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации; В-ПК-3[1] - владеть навыками организации и проведения мероприятий по контролю за обеспечением защиты информации, в том числе сведений, составляющих

	<p>деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.</p>		<p>государственную тайну, а также проведения анализа эффективности системы защиты информации</p>
<p>Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонент технических систем обеспечения безопасности информации; участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации; администрирование подсистем обеспечения информационной безопасности на объекте.</p>	<p>Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-</p>	<p>ПК-4 [1] - Способен способностью участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации</p> <p><i>Основание:</i> Профессиональный стандарт: 06.034</p>	<p>3-ПК-4[1] - знать основные нормативно-правовые акты и методические документы, содержащие требования к аттестационным испытаниям и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации, а также методы и методологию их проведения ; У-ПК-4[1] - уметь осуществлять аттестационные испытания и аттестации объектов, помещений,</p>

	<p>экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.</p>		<p>технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации; В-ПК-4[1] - владеть навыками участия в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации</p>
<p>Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонент технических систем обеспечения безопасности информации; участие в проведении специальных проверок</p>	<p>Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения</p>	<p>ПК-5 [1] - Способен осуществлять установку, настройку, эксплуатацию и администрирование компонентов технических систем обеспечения безопасности информации и поддержку их</p>	<p>З-ПК-5[1] - знать методологические основы и средства построения технических систем обеспечения безопасности информации, основы установки, настройки, эксплуатации и</p>

и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации; администрирование подсистем обеспечения информационной безопасности на объекте.	информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в	работоспособного состояния <i>Основание:</i> Профессиональный стандарт: 06.034	администрирования компонентов технических систем обеспечения безопасности информации и поддержки их работоспособного состояния ; У-ПК-5[1] - уметь осуществлять установку, настройку, эксплуатацию и администрирование компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния; В-ПК-5[1] - владеть методологией проведения установки, настройки, эксплуатации и администрирования компонентов технических систем обеспечения безопасности информации
--	--	--	--

	некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		
аналитический			
Получение и обработка поступающей информации; анализ и отбор данных и сведений для формирования информационных ресурсов; обработка акустических и видеозаписей, фотоматериалов с целью получения информации, необходимой для формирования ресурсов и оперативного реагирования; формирование автоматизированных, в том числе справочных, оперативно-розыскных, криминалистических учетов; осуществление информационного и оперативно-аналитического поиска; осуществление оперативно-розыскного анализа, идентификации, диагностики и прогнозирования, криминалистической диагностики; информационно-аналитическое обеспечение оперативно-розыскных	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели,	ПК-8 [1] - Способен применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование <i>Основание:</i> Профессиональный стандарт: 06.022	3-ПК-8[1] - знать ключевые методы аналитической разведки, методику проведения оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования ; У-ПК-8[1] - уметь применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; В-ПК-8[1] - владеть навыками определения необходимых механизмов для проведения аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования с учетом задач профессиональной деятельности

мероприятий и следственных действий; информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий; противодействие деструктивным и негативным информационно-психологическим воздействиям.	методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		
правоохранительный			
Обеспечение законности и правопорядка; предупреждение, выявление, пресечение, участие в раскрытии преступлений и иных правонарушений; информационно-аналитическое и информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий.	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-	ПК-10 [1] - Способен участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений <i>Основание:</i>	З-ПК-10[1] - знать основы уголовного, уголовно-процессуального права, криминалистики, криминологии ; У-ПК-10[1] - уметь оказывать содействие выявлению, предупреждению, пресечению, раскрытию и расследованию преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно

	<p>аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.</p>	<p>Анализ опыта: Выполнение деятельности в области выявления, предупреждения, пресечения, раскрытия и расследования преступлений.</p>	<p>использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений; В-ПК-10[1] - владеть навыками получения информации, ее анализа, оценки и использования в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений</p>
--	---	---	---

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 (B23)	профессионального модуля для формирования базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уровне пользователям.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за обеспечение кибербезопасности (B39)	1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий. 2.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования культуры решения изобретательских задач, развития логического мышления, путем погружения студентов в научную и инновационную деятельность института и вовлечения в проектную работу. 3.Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях. 4.Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное

		программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий. 5.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования системного подхода по обеспечению информационной безопасности и кибербезопасности в различных сферах деятельности посредством исследования и перенятия опыта постановки и решения научно-практических задач организациями-партнерами.
--	--	--

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практи. (семинары) / Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>8 Семестр</i>						
1	Причины трудоемкости решения задач защиты информации. Основы криптографии	1-8	16/8/8		25	КИ-8	3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-3, У-ПК-3, В-ПК-3, 3-ПК-4, У-ПК-4, В-ПК-4, 3-ПК-5, У-ПК-5, В-ПК-5, 3-ПК-8, У-ПК-8, В-ПК-8, 3-ПК-10,

							У-ПК-10, В-ПК-10
2	Разрушающие программные воздействия. Аппаратно- программные методы защиты информации	9-15	14/7/7		25	КИ-15	3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-3, У-ПК-3, В-ПК-3, 3-ПК-4, У-ПК-4, В-ПК-4, 3-ПК-5, У-ПК-5, В-ПК-5, 3-ПК-8, У-ПК-8, В-ПК-8, 3-ПК-10, У-ПК-10, В-ПК-10
	<i>Итого за 8 Семестр</i>		30/15/15		50		
	Контрольные мероприятия за 8 Семестр				50	3	3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-3, У-ПК-3, В-ПК-3, 3-ПК-4, У-ПК-4, В-ПК-4, 3-ПК-5, У-ПК-5, В-ПК-5, 3-ПК-8, У-ПК-8, В-ПК-8, 3-ПК-10, У-ПК-10, В-ПК-10

* – 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.
	<i>8 Семестр</i>	30	15	15
1-8	Причины трудоемкости решения задач защиты информации. Основы криптографии	16	8	8
1	Информационно-психологическая война. Информационно-техническая война. Главные угрозы кибербезопасности Информационно-психологическая война. Информационно-техническая война. Главные угрозы кибербезопасности. Источники угроз кибербезопасности. Политика коммерческих IT-компаний. Уязвимые IT-технологии. Сложность современных информационных систем. Все большее отстранение пользователей от реальных процессов управления и обработки информации. Человеческий фактор	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
2	Процессный подход к решению задач защиты информации Процессный подход к решению задач защиты информации. Стохастические методы защиты информации. Особенности криптографии как науки. Задачи, решаемые криптографическими методами. Стандарты криптографической защиты. Шифр Ф. Бэкона.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
3	Основные термины и определения. Правило Кергофса Основные термины и определения. Правило Кергофса. Требования к качественному шифру. Классификация шифров.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
4 - 5	Модель криптосистемы с секретным ключом. Блочные и поточные шифры Модель криптосистемы с секретным ключом. Блочные и поточные шифры. SP-сеть. Сеть Фейстеля. Архитектура Квадрат. XSL-шифры. Генераторы псевдослучайных чисел (ГПСЧ). Требования к качественному ГПСЧ. Хеш-функции. Требования к качественной хеш-функции.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
6 - 8	Модель криптосистемы с открытым ключом. Односторонняя функция, Односторонняя функция с секретом Модель криптосистемы с открытым ключом. Односторонняя функция, Односторонняя функция с секретом. Криптосистема RSA. Криптографические протоколы. Протокол выработки общего секретного ключа. Протокол классической электронной подписи. Протоколы аутентификации удаленных абонентов. Протокол разделения секрета. Протоколы доказательства с нулевым разглашением знаний.	Всего аудиторных часов		
		6	3	3
		Онлайн		
		0	0	0
9-15	Разрушающие программные воздействия. Аппаратно-программные методы защиты информации	14	7	7
9 - 10	Типы РПВ. Компьютерные вирусы (КВ), применяющие специальные приемы, затрудняющие их обнаружение Типы РПВ. Компьютерные вирусы (КВ), применяющие специальные приемы, затрудняющие их обнаружение.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0

	Сверхживучие КВ. Сетевые черви. Троянские программы. Бэкдоры. Эксплойты. Дропперы. Хакерские утилиты			
11	Методы антивирусной защиты (АВЗ) Методы антивирусной защиты (АВЗ). Комплекс программных средств АВЗ.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
12 - 13	Самотестирование СБИС. Контролепригодное проектирование Самотестирование СБИС. Контролепригодное проектирование. Контроль хода выполнения программ. Сторожевой процессор. Помехоустойчивое кодирование. Кодек (7, 4)-кода Хэмминга.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
14 - 15	Генераторы псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями Генераторы псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. Генераторы М-последовательностей. Генераторы (М - 1)-последовательностей. Генераторы (М + 1)-последовательностей.	Всего аудиторных часов		
		4	2	2
		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

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	Темы занятий / Содержание
	<i>8 Семестр</i>
5	Криптоанализ шифра "Усложненная перестановка по таблице" Криптоанализ шифра "Усложненная перестановка по таблице".
6	Протокол электронной подписи Протокол электронной подписи.
7	Протокол выработки общего секретного ключа Протокол выработки общего секретного ключа.
8 - 9	Протоколы аутентификации удаленных абонентов Протоколы аутентификации удаленных абонентов.
10	Протокол доказательства с нулевым разглашением знаний Протокол доказательства с нулевым разглашением знаний.

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	Темы занятий / Содержание
	<i>8 Семестр</i>
1 - 8	Причины трудоемкости решения задач защиты информации. Основы криптографии Причины трудоемкости решения задач защиты информации. Основы криптографии
9 - 15	Разрушающие программные воздействия. Аппаратно-программные методы защиты информации Разрушающие программные воздействия. Аппаратно-программные методы защиты информации

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При чтении лекционного материала используется электронное сопровождение курса: справочно-иллюстративный материал воспроизводится и озвучивается в аудитории с использованием проектора и переносного компьютера в реальном времени. Электронный материал доступен студентам для использования и самостоятельного изучения на сайте кафедры.

На сайте кафедры также находится методический и справочный материал, необходимый для проведения лабораторного практикума по курсу.

Лабораторный практикум проводится по расписанию в дисплейном классе одновременно для группы студентов, работающих в интерактивном режиме. Допустимо выполнение лабораторных работ в составе локальной сети кафедры или в удаленном режиме, используя Интернет.

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-1	З-ПК-1	З, КИ-8, КИ-15
	У-ПК-1	З, КИ-8, КИ-15
	В-ПК-1	З, КИ-8, КИ-15
ПК-10	З-ПК-10	З, КИ-8, КИ-15
	У-ПК-10	З, КИ-8, КИ-15
	В-ПК-10	З, КИ-8, КИ-15
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	З-ПК-4	З, КИ-8, КИ-15
	У-ПК-4	З, КИ-8, КИ-15
	В-ПК-4	З, КИ-8, КИ-15
ПК-5	З-ПК-5	З, КИ-8, КИ-15

ПК-8	У-ПК-5	3, КИ-8, КИ-15
	В-ПК-5	3, КИ-8, КИ-15
	3-ПК-8	3, КИ-8, КИ-15
	У-ПК-8	3, КИ-8, КИ-15
	В-ПК-8	3, 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 излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
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.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Г 55 Введение в теоретико-числовые методы криптографии : , Круглов И. А. [и др.], Санкт-Петербург: Лань, 2022
2. ЭИ В 60 Защита информации : учебное пособие для вузов, Внуков А. А., Москва: Юрайт, 2023
3. ЭИ И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, Иванов М.А., Чугунков И.В., Москва: НИЯУ МИФИ, 2012
4. ЭИ Ч-45 Применение искусственных нейронных сетей и системы остаточных классов в криптографии : учебное пособие, Лавриненко И. Н. [и др.], Москва: Физматлит, 2012
5. ЭИ Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, Шустова Л.И. [и др.], Москва: НИЯУ МИФИ, 2011

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 519 С13 Введение в алгебраические коды : учебное пособие, Сагалович Ю.Л., Москва: ИППИ, 2010
2. 004 П64 Поточные шифры : , Рузин А.В. [и др.], М.: Кудиц-образ, 2003
3. 004 Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, Шустова Л.И. [и др.], Москва: НИЯУ МИФИ, 2011
4. 004 Ш76 Секреты и ложь : Безопасность данных в цифровом мире, Шнайер Б., М.и др.: Питер, 2003
5. 0 М24 Современная криптография : теория и практика, Мао В., Москва [и др.]: Вильямс, 2005
6. 004 И20 Теория, применение и оценка качества генераторов псевдослучайных последовательностей : , Иванов М.А., Чугунков И.В., Москва: Кудиц-образ, 2003
7. 004 Г82 Цифровая стеганография : , Оков И.Н., Туринцев И.В., Грибунин В.Г., М.: Солон-Пресс, 2002

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

1. Указания для прослушивания лекций

Перед началом занятий ознакомиться с учебным планом и списком рекомендованной литературы.

Перед посещением очередной лекции освежить в памяти основные концепции пройденного ранее материала. Подготовить при необходимости вопросы преподавателю. На каждой лекции следует задавать вопросы как по материалу текущей лекции, так и по ранее прочитанным лекциям.

При изучении лекционного материала обязательно следует сопоставлять его с материалом семинарских и лабораторных занятий.

Для более подробного изучения курса следует работать с рекомендованными литературными источниками и материалами из сети Internet.

2. Указания для проведения лабораторного практикума.

Соблюдать требования техники безопасности, для чего прослушать необходимые разъяснения о правильности поведения в лаборатории.

Перед выполнением лабораторной работы провести самостоятельно подготовку к работе изучив основные теоретические положения, знание которых необходимо для осмысленного выполнения работы.

В процессе выполнения работы следует постоянно общаться с преподавателем, не допуская по возможности неправильных действий.

При сдаче зачета по работе подготовить отчет о проделанной работе, где должны быть отражены основные результаты и выводы.

3. Указания по выполнению самостоятельной работы

Получить у преподавателя задание и список рекомендованной литературы.

Изучение теоретических вопросов следует проводить по возможности самостоятельно, но при затруднениях обращаться к преподавателю.

При выполнении фронтальных заданий по усмотрению преподавателя работа может быть оценена без письменного отчета на основе ответов на контрольные вопросы, при условии активной самостоятельной работы.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

1. Указания для проведения лекций

На первой вводной лекции сделать общий обзор содержания курса. Дать перечень рекомендованной основной литературы и вновь появившихся литературных источников.

Перед изложением текущего лекционного материала кратко напомнить об основных выводах по материалам предыдущей лекции.

Внимательно относиться к вопросам студентов и при необходимости давать дополнительные более подробные пояснения.

Периодически освещать на лекциях наиболее важные вопросы лабораторного практикума, вызывающие у студентов затруднения.

В середине семестра (ориентировочно после 8-й лекции) обязательно провести контроль знаний студентов по материалам всех прочитанных лекций.

Желательно использовать конспекты лекций, в которых используется принятая преподавателем система обозначений.

Давать рекомендации студентам для подготовки к очередным лабораторным работам.

На последней лекции уделить время для обзора наиболее важных положений, рассмотренных в курсе.

2. Указания для проведения лабораторного практикума

На первом занятии рассказать о лабораторном практикуме в целом (о целях практикума, инструментальных средствах для выполнения лабораторных работ, о порядке отчета по лабораторным работам), провести инструктаж по технике безопасности при работе в лаборатории.

Для выполнения каждой лабораторной работы студентам выдавать индивидуальные задания.

При принятии отчета по каждой лабораторной работе обязательно побеседовать с каждым студентом, задавая контрольные вопросы, направленные на понимание изучаемой в лабораторной работе проблемы.

По каждой работе фиксировать факт выполнения и ответа на контрольные вопросы.

Общий зачет по практикуму должен включать все зачеты по каждой лабораторной работе в отдельности.

Задания на каждую следующую лабораторную работу студенту выдавать по мере выполнения и сдачи предыдущих работ.

Автор(ы):

Иванов Михаил Александрович, д.т.н., профессор

Рецензент(ы):

Чугунков И.В.