

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-2

от 31.05.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
СОВРЕМЕННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ И ИХ БЕЗОПАСНОСТЬ

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, экс./зач./КР/КП
8	2	72	30	0	15	27	0	3
Итого	2	72	30	0	15	0	27	0

АННОТАЦИЯ

Формирование принципов построения электронных платежных систем

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения дисциплины является изучение принципов построения электронных платежных систем.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Для успешного освоения дисциплины от обучаемого требуются:

- знать основы криптографической защиты информации;

Настоящая дисциплина должна предшествовать УИР и КП.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-3 [1] – Способен использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	З-ОПК-3 [1] – знать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач У-ОПК-3 [1] – уметь использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач В-ОПК-3 [1] – владеть навыками определения релевантных общенаучных методов, законов физики, математического аппарата, методов моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач
ОПК-4 [1] – Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	З-ОПК-4 [1] – знать принципы создания и функционирования систем обеспечения информационной безопасности, основные нормативные и методические документы в области защиты информации, методику обоснования проектных решений, разработки рабочей технической документации У-ОПК-4 [1] – уметь выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации

	В-ОПК-4 [1] – владеть методикой обоснования проектных решений, а также навыками разработки, оформления, представления рабочей технической документации в соответствии с действующими нормативными и методическими документами в области защиты информации
ОПК-5 [1] – Способен планировать проведение работ по комплексной защите информации на объекте информатизации	З-ОПК-5 [1] – знать основные принципы, правила, процедуры, практические приемы, методы, средства применяемые для обеспечения комплексной защиты информации на объекте информатизации У-ОПК-5 [1] – уметь планировать и проводить работы по комплексной защите информации на объекте информатизации В-ОПК-5 [1] – владеть навыками и стратегиями планирования работ по комплексной защите информации на объекте информатизации
ОПК-6 [1] – Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач	З-ОПК-6 [1] – знать основы теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи У-ОПК-6 [1] – уметь применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач В-ОПК-6 [1] – владеть методами цифровой обработки сигналов, информации и кодирования, электрической связи
ОПК-7 [1] – Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач	З-ОПК-7 [1] – знать основные программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач У-ОПК-7 [1] – уметь применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач В-ОПК-7 [1] – владеть навыками освоения новых программных средств системного и прикладного назначения, языков, методов и инструментальных средств программирования для решения профессиональных задач

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	Код и наименование индикатора достижения профессиональной
---	----------------------------------	---	--

		(профессиональный стандарт-ПС, анализ опыта)	компетенции
	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 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-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-	ПК-6 [1] - Способен формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы <i>Основание:</i> Профессиональный стандарт: 06.011	З-ПК-6[1] - знать основные информационно-поисковые и логико-аналитические системы и принципы работы с ними, а также теоретические основы баз данных, структуру баз данных, системы управления базами данных для информационных систем различного назначения, архитектуру баз данных, физические и логические уровни представления данных, основы моделей данных, основы проектирования баз данных ; У-ПК-6[1] - уметь формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические; В-ПК-6[1] - владеть принципами разработки и создания автоматизированных баз и банков данных, а также принципами их использования

<p>информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий; противодействие деструктивным и негативным информационно-психологическим воздействиям.</p>	<p>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>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</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</p>	<p>ПК-7 [1] - Способен анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности</p> <p><i>Основание:</i> Профессиональный стандарт: 06.033</p>	<p>З-ПК-7[1] - знать основы работы с информационными массивами и информационными процессами на предмет выявления угроз безопасности ; У-ПК-7[1] - уметь анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности; В-ПК-7[1] - владеть навыками проведения различных видов анализа, методикой выявления угроз безопасности информационных массивов и информационных процессов</p>

<p>информационного и оперативно-аналитического поиска; осуществление оперативно-розыскного анализа, идентификации, диагностики и прогнозирования, криминалистической диагностики; информационно-аналитическое обеспечение оперативно-розыскных мероприятий и следственных действий; информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий; противодействие деструктивным и негативным информационно-психологическим воздействиям.</p>	<p>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>Получение и обработка поступающей информации; анализ и отбор данных и сведений для формирования информационных</p>	<p>Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты</p>	<p>ПК-8 [1] - Способен применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-</p>	<p>3-ПК-8[1] - знать ключевые методы аналитической разведки, методику проведения оперативно-аналитического поиска, оперативно-</p>

<p>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 мероприятий и следственных действий; информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий; противодействие деструктивным и негативным информационно-</p>	<p>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 деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового</p>	<p>розыскной анализ, идентификацию, диагностику, прогнозирование</p> <p><i>Основание:</i> Профессиональный стандарт: 06.022</p>	<p>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</p>
--	---	---	---

психологическим воздействиям.	мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		
-------------------------------	---	--	--

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (B18)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (B19)	1. Использование воспитательного потенциала дисциплин/практик «Научно-исследовательская работа», «Проектная практика», «Научный семинар» для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2. Использование воспитательного потенциала дисциплин "История науки и инженерии", "Критическое мышление и основы научной коммуникации", "Введение в специальность", "Научно-исследовательская работа", "Научный семинар" для:

		<p>- формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед;</p> <p>- формирования критического мышления, умения рассматривать различные исследования с экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок появления тех или иных открытий и теорий.</p>
<p>Профессиональное воспитание</p>	<p>Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (B40)</p>	<p>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.</p> <p>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.</p> <p>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</p>

		<p>лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях.</p> <p>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.</p> <p>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.</p>
--	--	--

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
	<i>8 Семестр</i>						
1	Основы защиты компьютерной информации. Традиционная и электронная	1-5	10/0/5		25	КИ-5	3-ОПК-3, У-ОПК-

	коммерция						3, В- ОПК- 3, 3- ОПК- 4, У- ОПК- 4, В- ОПК- 4, 3- ОПК- 5, У- ОПК- 5, В- ОПК- 5, 3- ОПК- 6, У- ОПК- 6, В- ОПК- 6, 3- ОПК- 7, У- ОПК- 7, В- ОПК- 7, 3-ПК- 6, У- ПК-6, В- ПК-6, 3-ПК- 7, У- ПК-7, В- ПК-7,
--	-----------	--	--	--	--	--	--

							З-ПК-8, У-ПК-8, В-ПК-8
2	Особенности реализации электронных систем с использованием платежных карт	6-10	10/0/5		25	КИ-10	З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ОПК-4, У-ОПК-4, В-ОПК-4, З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ОПК-6, У-ОПК-6, В-ОПК-6, З-ОПК-7, У-ОПК-7, В-ОПК-7, З-ПК-

							6, У- ПК-6, В- ПК-6, З-ПК- 7, У- ПК-7, В- ПК-7, З-ПК- 8, У- ПК-8, В- ПК-8
3	Дематериализованные средства платежа. Российские платежные системы	11-15	10/0/5		25	КИ-15	В- ОПК- 4, З- ОПК- 5, У- ОПК- 5, В- ОПК- 5, З- ОПК- 6, У- ОПК- 6, В- ОПК- 6, З- ОПК- 7, У- ОПК- 7, В- ОПК- 7, З-ПК- 6, У- ПК-6, В-

							ПК-6, З-ПК-7, У-ПК-7, В-ПК-7, З-ПК-8, У-ПК-8, В-ПК-8, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ОПК-4, У-ОПК-4
	<i>Итого за 8 Семестр</i>		30/0/15		75		
	Контрольные мероприятия за 8 Семестр				25	3	З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ОПК-4, У-ОПК-4, В-ОПК-6, З-ОПК-7, У-ОПК-

							7, В- ОПК- 7, З-ПК- 6, У- ПК-6, В- ПК-6, З-ПК- 7, У- ПК-7, В- ПК-7, З-ПК- 8, У- ПК-8, В- ПК-8, В- ОПК- 4, З- ОПК- 5, У- ОПК- 5, В- ОПК- 5, З- ОПК- 6, У- ОПК- 6
--	--	--	--	--	--	--	--

* – 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

Недел и	Темы занятий / Содержание	Лек., час.	Пр./сем. , час.	Лаб., час.
	<i>8 Семестр</i>	30	0	15
1-5	Основы защиты компьютерной информации. Традиционная и электронная коммерция	10	0	5
1	Угрозы безопасности информационных систем. Типы атак на протоколы информационного взаимодействия. Службы защиты. Криптографические методы защиты. Классификация методов шифрования информации. Криптосистемы с секретным ключом. Криптосистемы с открытым ключом.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
2	Криптографические протоколы. Контроль целостности информации. Методы аутентификации информации. Электронная подпись. Слепая электронная подпись. Вероятностное шифрование.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
3	Традиционная и электронная коммерции. Виды электронной коммерции: B2B, B2C, C2C, P2P. Платежные системы. Интернет-банкинг. Мобильная коммерция. Протокол WAP. Информационная безопасность электронного бизнеса.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
4	Механизмы классических денег. Платежные средства. Типы дематериализованных денег. Электронные деньги. Виртуальные деньги. Цифровые деньги. Электронные и виртуальные кошельки. Электронные и виртуальные жетоны. Транзакционные свойства дематериализованных валют. Анонимность и неотслеживаемость платежей.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
5	Классификация и области использования микропроцессорных карт. Карты с контактной площадкой. Безопасность микропроцессорных карт. Физическая и логическая безопасность. Атаки на смарт-карты. Многоцелевые смарт-карты. Файловые системы смарт-карт. Стандартизация микропроцессорных карт. ISO 7816.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
6-10	Особенности реализации электронных систем с использованием платежных карт	10	0	5
6	Удаленные платежи при помощи банковский карт. Протоколы iKP. CyberCash	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
7	Протокол SSL.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
8	Протокол SET.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
9	Системы проведения микроплатежей и face-to-face коммерция. Характеристики систем проведения	Всего аудиторных часов		
		2	0	1

	микроплатежей. Chipper. GeldKarte. Mondex.	Онлайн	0	0	0
10	Удаленные микроплатежи. NetBill. KleLine. MilliCent. Цифровые облигации.	Всего аудиторных часов	2	0	1
		Онлайн	0	0	0
			10	0	5
11-15	Дематериализованные средства платежа. Российские платежные системы				
11	Цифровые деньги. Строительные блоки. Неотслеживаемость покупателя и продавца. Номинал цифровых купюр. Обнаружение подделки.	Всего аудиторных часов	2	0	1
		Онлайн	0	0	0
12	Электронные чеки. Классический процесс обработки бумажных чеков. Электронные чеки. Формат электронного чека. NetCheque.	Всего аудиторных часов	2	0	1
		Онлайн	0	0	0
13	Платформы и модели объединения платежных систем. Архитектура Semper. Cafe. Карты продавцов и банков.	Всего аудиторных часов	2	0	1
		Онлайн	0	0	0
14	Платежные системы, используемые в России. Электронные межбанковские расчеты. Системы Клиент-Банк. CyberPlat. PayCash. WebMoney.	Всего аудиторных часов	2	0	1
		Онлайн	0	0	0
15	Перспективы развития платежных систем. Стандартизация платежных систем.	Всего аудиторных часов	2	0	1
		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>
	Основы защиты компьютерной информации. Традиционная и электронная коммерция Основы защиты компьютерной информации. Традиционная и электронная коммерция

	Особенности реализации электронных систем с использованием платежных карт Особенности реализации электронных систем с использованием платежных карт
	Дематериализованные средства платежа. Российские платежные системы Дематериализованные средства платежа. Российские платежные системы

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)
ОПК-3	З-ОПК-3	З, КИ-5, КИ-10, КИ-15
	У-ОПК-3	З, КИ-5, КИ-10, КИ-15
	В-ОПК-3	З, КИ-5, КИ-10, КИ-15
ОПК-4	З-ОПК-4	З, КИ-5, КИ-10, КИ-15
	У-ОПК-4	З, КИ-5, КИ-10, КИ-15
	В-ОПК-4	З, КИ-5, КИ-10, КИ-15
ОПК-5	З-ОПК-5	З, КИ-5, КИ-10, КИ-15
	У-ОПК-5	З, КИ-5, КИ-10, КИ-15
	В-ОПК-5	З, КИ-5, КИ-10, КИ-15
ОПК-6	З-ОПК-6	З, КИ-5, КИ-10, КИ-15
	У-ОПК-6	З, КИ-5, КИ-10, КИ-15
	В-ОПК-6	З, КИ-5, КИ-10, КИ-15
ОПК-7	З-ОПК-7	З, КИ-5, КИ-10, КИ-15
	У-ОПК-7	З, КИ-5, КИ-10, КИ-15
	В-ОПК-7	З, КИ-5, КИ-10, КИ-15

ПК-6	З-ПК-6	З, КИ-5, КИ-10, КИ-15
	У-ПК-6	З, КИ-5, КИ-10, КИ-15
	В-ПК-6	З, КИ-5, КИ-10, КИ-15
ПК-7	З-ПК-7	З, КИ-5, КИ-10, КИ-15
	У-ПК-7	З, КИ-5, КИ-10, КИ-15
	В-ПК-7	З, КИ-5, КИ-10, КИ-15
ПК-8	З-ПК-8	З, КИ-5, КИ-10, КИ-15
	У-ПК-8	З, КИ-5, КИ-10, КИ-15
	В-ПК-8	З, КИ-5, КИ-10, 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 – <i>«отлично»</i>	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 – <i>«хорошо»</i>	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 – <i>«удовлетворительно»</i>	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 – <i>«неудовлетворительно»</i>	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

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ L69 Banking on Innovation : Modernisation of Payment Systems, Heidelberg: Physica-Verlag HD,, 2009
2. ЭИ 3-31 Криптографические методы защиты информации : учебник для вузов, Москва: Юрайт, 2022
3. ЭИ Ф 76 Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов, Москва: Юрайт, 2022
4. ЭИ И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, Москва: НИЯУ МИФИ, 2012
5. ЭИ Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, ред. М. А. Иванов, Москва: НИЯУ МИФИ, 2011

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, А. Б. Вавренюк [и др.], Москва: НИЯУ МИФИ, 2011
2. 004 С82 Стохастические методы и средства защиты информации в компьютерных системах и сетях : , М. А. Иванов [и др.] ; ред. : И. Ю. Жуков, Москва: Кудиц-Пресс, 2009
3. 004 И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, М. А. Иванов, И. В. Чугунков ; ред. : М. А. Иванов, Москва: НИЯУ МИФИ, 2012
4. 004 П30 Основы практической защиты информации : Учеб.пособие, Петраков А.В., М.: Радио и связь, 2000
5. 004 Р69 Безопасность информации в автоматизированных системах банковских расчетов : , Романов М.Ю.,Скородумов Б.И., М.: МИФИ, 1998
6. 0 3-31 Криптографические протоколы и их применение в финансовой и коммерческой деятельности : учебное пособие для вузов, С. В. Запечников, Москва: Горячая линия-Телеком, 2007
7. 004 Д73 Информационные системы и процессы : Учеб. пособие, Ю. Г. Древис, М.: МИФИ, 2003

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Кафедра "Компьютерные системы и технологии" (<http://dozen.mephi.ru>)

<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 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.

у. 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.

3. Указания по контролю самостоятельной работы студентов

Контроль самостоятельной работой студентов осуществлять в процессе приема лабораторных работ, при проведении индивидуальных консультаций, а также при чтении лекций на неделе семестрового контроля.

Для самостоятельной работы студентов предоставлять в согласованное время учебные лаборатории.

Автор(ы):

Чугунков Илья Владимирович

Рецензент(ы):
Иванов М.А.