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 ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность) — [1] 09.04.01 Информатика и вычислительная техника

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**
1	3-5	108-180	32	0	16		24-96	0	Э
Итого	3-5	108-180	32	0	16	0	24-96	0	

Москва, 2020

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

Дисциплина Защита информации относится к базовой части рабочего учебного плана.

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
ОПК-1 [1] – Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	З-ОПК-1 [1] – Знать: основы математики, физики, социально-экономических наук, вычислительной техники и программирования У-ОПК-1 [1] – Уметь: решать нестандартные профессиональные задачи с применением естественнонаучных, общеинженерных и социально-экономических знаний В-ОПК-1 [1] – Владеть: навыками решения нестандартных задач профессиональной деятельности, в том числе в междисциплинарном контексте
ОПК-2 [1] – Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	З-ОПК-2 [1] – Знать: современные информационные и интеллектуальные технологии и инструментальные средства разработки алгоритмов и программного обеспечения, алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения У-ОПК-2 [1] – Уметь: выбирать современные информационные и интеллектуальные технологии и инструментальные средства разработки алгоритмов и программного обеспечения, составлять алгоритмы, писать и отлаживать коды на языке программирования, тестировать работоспособность программы,

	интегрировать программные модули В-ОПК-2 [1] – Владеть: навыками применения современных информационных и интеллектуальных технологий и инструментальных средств разработки алгоритмов и программного обеспечения, языками программирования, навыками отладки и тестирования работоспособности программ, применяемых для решения профессиональных задач
ОПК-3 [1] – Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	З-ОПК-3 [1] – Знать: принципы, методы и средства анализа профессиональной информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У-ОПК-3 [1] – Уметь: анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности В-ОПК-3 [1] – Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с применением информационно-коммуникационных технологий с учетом требований информационной безопасности
ОПК-4 [1] – Способен применять на практике новые научные принципы и методы исследований	З-ОПК-4 [1] – Знать: новые научные принципы и методы исследований в рамках своей профессиональной деятельности и в смежных областях У-ОПК-4 [1] – Уметь: применять на практике новые научные принципы и методы исследований В-ОПК-4 [1] – Владеть: навыками применения методов современных научных исследований
ОПК-5 [1] – Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	З-ОПК-5 [1] – Знать: современные информационные технологии и инструментальные средства разработки программного и аппаратного обеспечения информационных и автоматизированных систем У-ОПК-5 [1] – Уметь: выбирать и применять современные инструментальные средства разработки программного и аппаратного обеспечения информационных и автоматизированных систем в соответствии с решаемыми задачами В-ОПК-5 [1] – Владеть: навыками разработки и модернизации программного и аппаратного обеспечения информационных и автоматизированных систем с применением современных инструментальных средств
ОПК-6 [1] – Способен разрабатывать компоненты	З-ОПК-6 [1] – Знать: современные информационные технологии и инструментальные средства разработки

программно-аппаратных комплексов обработки информации и автоматизированного проектирования	программно-аппаратных комплексов обработки информации и автоматизированного проектирования У-ОПК-6 [1] – Уметь: выбирать и применять современные информационные технологии и инструментальные средства разработки программно-аппаратных комплексов обработки информации и автоматизированного проектирования в соответствии с решаемыми задачами В-ОПК-6 [1] – Владеть: навыками разработки компонентов программно-аппаратных комплексов обработки информации и автоматизированного проектирования
ОПК-7 [1] – Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий	З-ОПК-7 [1] – Знать: современные информационные технологии и инструментальные средства разработки комплексов обработки информации и автоматизированного проектирования У-ОПК-7 [1] – Уметь: анализировать технические характеристики зарубежных комплексов обработки информации и автоматизированного проектирования, выбирать и применять современные информационные технологии и инструментальные средства разработки комплексов обработки информации и автоматизированного проектирования с целью адаптации данных комплексов к нуждам отечественных предприятий В-ОПК-7 [1] – Владеть: навыками адаптации зарубежных комплексов обработки информации и автоматизированного проектирования к нуждам отечественных предприятий
ОПК-8 [1] – Способен осуществлять эффективное управление разработкой программных средств и проектов	З-ОПК-8 [1] – Знать: действующее законодательство в области управления разработкой программных средств и проектов, цели, принципы, функции, объекты управления проектами, основные инструменты проведения реинжиниринга бизнес-процессов, методы сбора информации, подходы к организации деятельности специфических служб по управлению проектами, основные методологии управления проектами У-ОПК-8 [1] – Уметь: проектировать организационную структуру, осуществлять распределение полномочий и ответственности на основе их делегирования В-ОПК-8 [1] – Владеть: современными инструментальными средствами по управлению проектами, навыками организации деятельности по управлению проектами, методами оценки эффективности
УК-4 [1] – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и	З-УК-4 [1] – Знать: правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном языках; существующие профессиональные сообщества для профессионального взаимодействия

профессионального взаимодействия	У-УК-4 [1] – Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия В-УК-4 [1] – Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий
УКЦ-1 [1] – Способен решать исследовательские, научно-технические и производственные задачи в условиях неопределенности, в том числе выстраивать деловую коммуникацию и организовывать работу команды с использованием цифровых ресурсов и технологий в цифровой среде	З-УКЦ-1 [1] – Знать современные цифровые технологии, используемые для выстраивания деловой коммуникации и организации индивидуальной и командной работы У-УКЦ-1 [1] – Уметь подбирать наиболее релевантные цифровые решения для достижения поставленных целей и задач, в том числе в условиях неопределенности В-УКЦ-1 [1] – Владеть навыками решения исследовательских, научно-технических и производственных задач с использованием цифровых технологий
УКЦ-2 [1] – Способен к самообучению, самоактуализации и саморазвитию с использованием различных цифровых технологий в условиях их непрерывного совершенствования	З-УКЦ-2 [1] – Знать основные цифровые платформы, технологи и интернет ресурсы используемые при онлайн обучении У-УКЦ-2 [1] – Уметь использовать различные цифровые технологии для организации обучения В-УКЦ-2 [1] – Владеть навыками самообучения, самооактулизации и саморазвития с использованием различных цифровых технологий

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 достижени профессиональной компетенции**
научно-исследовательский и инновационный			
Разработка рабочих планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей. Сбор, обработка, анализ и систематизация научно-технической информации по теме исследования,	Вычислительные машины, комплексы, системы и сети. Автоматизированные системы обработки информации и управления. Системы автоматизированного проектирования и информационной поддержки	ПК-1 [1] - Способен применять научно обоснованные перспективные методы исследования и решать задачи на основе знания мировых тенденций развития вычислительной техники и информационных технологий с внедрением результатов исследований	З-ПК-1[1] - Знать: мировые тенденции развития вычислительно техники и информационных технологий, современны методы научных исследований, действующее законодательство в области интеллектуальной

выбор методик и средств решения задачи. Разработка математических моделей исследуемых процессов и изделий. Разработка методик проектирования новых процессов и изделий. Разработка методик автоматизации принятия решений. Организация проведения экспериментов и испытаний, анализ их результатов. Подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований. Внедрение результатов научно-технических исследований в реальный сектор экономики и коммерциализации разработок.	жизненного цикла промышленных изделий. Программное обеспечение средств вычислительной техники и автоматизированных систем (программы, программные комплексы и системы). Математическое, информационное, техническое, лингвистическое, программное, эргономическое, организационное и правовое обеспечение перечисленных систем.	в реальный сектор экономики *Основание:* Профессиональный стандарт: 06.014, 06.022	собственности ; У-ПК-1[1] - Уметь: выбирать современные информационные технологии, научно обоснованные перспективные методы исследования и программные средства, том числе отечественно производства при решении задач профессиональной деятельности, внедрять результаты исследовани в реальный сектор экономики; В-ПК-1[1] - Владеть: навыками применения научно обоснованных перспективных методов исследования и решения задач на основе знания мировых тенденций развития вычислительно техники и информационных технологий с внедрение результатов исследовани в реальный сектор экономики
производственно-технологической			
Проектирование и применение инструментальных средств реализации программно-аппаратных проектов. Разработка методик реализации и сопровождения программных продуктов. Разработка технических заданий на проектирование программного обеспечения для средств управления и технологического оснащения промышленного производства и их реализация с помощью	Вычислительные машины, комплексы, системы и сети. Автоматизированные системы обработки информации и управления. Системы автоматизированного проектирования и информационной поддержки жизненного цикла промышленных изделий. Программное обеспечение средств вычислительной техники и автоматизированных	ПК-2 [1] - Способен разрабатывать модели и компоненты высокопроизводительного защищенного программно-аппаратного обеспечения и автоматизированных систем обработки информации и управления с использованием современных инструментальных средств и технологий *Основание:* Профессиональный стандарт: 06.015, 06.022, 06.028	З-ПК-2[1] - Знать: современные информационные технологии и инструментальные средства разработки моделей и компонентов высокопроизводительно защищенного программно-аппаратног обеспечения и автоматизированных систем обработки информации и управления ; У-ПК-2[1] - Уметь: выбирать и применять современные информационные технологии и

средств автоматизированного проектирования. Тестирование программных продуктов и баз данных. Выбор систем обеспечения экологической безопасности производства. Проведение испытаний, внедрение и ввод в эксплуатацию разработанных программно-аппаратных комплексов, баз данных, информационных систем и автоматизированных систем обработки информации и управления. Использование передовых методов оценки качества, надежности и информационной безопасности программно-аппаратных комплексов, баз данных, информационных систем и автоматизированных систем обработки информации и управления. Использование информационных сервисов для автоматизации прикладных и информационных процессов предприятий высокотехнологических отраслей экономики.	систем (программы, программные комплексы и системы). Математическое, информационное, техническое, лингвистическое, программное, эргономическое, организационное и правовое обеспечение перечисленных систем.		инструментальные средства разработки моделей и компонентов высокопроизводительно защищенного программно-аппаратног обеспечения и автоматизированных систем обработки информации и управления в соответствии с решаемыми задачами; В-ПК-2[1] - Владеть: навыками разработки моделей и компонентов высокопроизводительно защищенного программно-аппаратног обеспечения и автоматизированных систем обработки информации и управления с использованием современных инструментальных средств и технологий
организационно-управленческий			
организация работы коллектива исполнителей, принятие исполнительских решений в условиях спектра мнений, определение порядка выполнения работ; поиск оптимальных решений	Автоматизированные системы обработки информации и управления	ПК-3 [1] - Способен организовывать работу и руководить коллективами разработчиков в области информатики и вычислительной техники *Основание:*	З-ПК-3[1] - Знать: действующее законодательство в области информатики и вычислительной техник управления разработкой проектов, цели, принципы, функции, объекты управления

при создании продукции с учетом требований качества, надежности и стоимости, а также сроков исполнения, безопасности жизнедеятельности и экологической чистоты; организация в подразделениях работы по совершенствованию, модернизации, унификации компонентов программного, лингвистического и информационного обеспечения и по разработке проектов стандартов и сертификатов; адаптация современных версий систем управления качеством к конкретным условиям производства на основе международных стандартов; поддержка единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции; планирование перспективных и конкурентоспособных разработок в области высокопроизводительного защищенного программно-аппаратного обеспечения и автоматизированных систем обработки информации и управления.		Профессиональный стандарт: 06.016	проектами, основные инструменты проведени реинжиниринга бизнес-процессов, методы сбор информации, подходы к организации деятельнос специфических служб п управлению проектами, основные методологии управления проектами У-ПК-3[1] - Уметь: организовывать работу и руководить коллективам разработчиков в области информатики и вычислительной техник В-ПК-3[1] - Владеть: навыками организации работы и руководства коллективами разработчиков в области информатики и вычислительной техник с оценкой эффективност их деятельности
проектный			
разработка планов работ по автоматизации предприятий и организаций; подготовка заданий на разработку проектных решений;	Автоматизированные системы обработки информации и управления	ПК-4 [1] - Способен разрабатывать, согласовывать и выпускать все виды проектной документации	З-ПК-4[1] - Знать: требования ГОСТ ЕСКД ЕСТД и ЕСПД по разработке и выпуску всех видов проектной документации в области

разработка проектов автоматизированных систем различного назначения, обоснование выбора аппаратно-программных средств автоматизации и информатизации предприятий и организаций; концептуальное проектирование сложных изделий, включая программные комплексы, с использованием средств автоматизации проектирования, передового опыта разработки конкурентоспособных изделий; выполнение проектов по созданию программ, баз данных и комплексов программ автоматизированных информационных систем; разработка и реализация проектов по интеграции информационных систем в соответствии с методиками и стандартами информационной поддержки изделий, включая методики и стандарты документооборота, интегрированной логистической поддержки, оценки качества программ и баз данных, электронного бизнеса проведение технико-экономического и функционально-стоимостного анализа эффективности проектируемых систем; разработка методических и нормативных документов, технической документации, а также		*Основание:* Профессиональный стандарт: 06.015, 06.019	информатики и вычислительной техник У-ПК-4[1] - Уметь: выполнять разработку, согласование и выпуск всех видов проектной документации; В-ПК-4[1] - Владеть: современными инструментальными средствами по разработ и выпуску проектной документации

предложений и мероприятий по реализации разработанных проектов и программ			

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
	1 Семестр						
1	Защита информации от умышленных деструктивных воздействий	1-8			25	КИ-8	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, 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-ОПК-8, У-ОПК-8, В-ОПК-8, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-4,

							У-УК-4, В-УК-4, З-УКЦ-1, У-УКЦ-1, В-УКЦ-1, З-УКЦ-2, У-УКЦ-2, В-УКЦ-2, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-4
2	Защита информации от случайных деструктивных воздействий	9-16			25	КИ-16	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2,

							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-ОПК-8, У-ОПК-8, В-

							ОПК-8, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-4, У-УК-4, В-УК-4, З-УКЦ-1, У-УКЦ-1, В-УКЦ-1, З-УКЦ-2, У-УКЦ-2, В-УКЦ-2, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-4
	Итого за 1 Семестр		32/0/16		50		
	Контрольные				50	Э	З-

	мероприятия за 1 Семестр						ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, 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-ОПК-8, У-ОПК-8, В-ОПК-8, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-4, У-УК-4, В-УК-4, З-УКЦ-1, У-УКЦ-1, В-УКЦ-1, З-УКЦ-2, У-УКЦ-2,

							В-УКЦ-2, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-4

* – 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.**
	1 Семестр	32	0	16
1-8	**Защита информации от умышленных деструктивных воздействий**	16		8
1	Компьютерные системы (КС) как объекты защиты информации. Методы и средства защиты информации от случайных и преднаме-ренных деструктивных воздействий. Требования к эффективной системе обеспечения безопасности информации (ОБИ).	Всего аудиторных часов		
		2		1
		Онлайн		
2	Введение в криптологию. Основные термины и определения. Криптографическое преобразование информации. Классификация шифров. Требования к качественному шифру. Требования к каче-ственной хеш-функции.	Всего аудиторных часов		
		2		1
		Онлайн		
3	Криптосистемы с секретным ключом. ГОСТ 28147-89. Американ-ский стандарт криптозащиты AES-128. Поточные шифры A5, RC4.	Всего аудиторных часов		
		2		1
		Онлайн		
4 - 5	Криптосистемы с открытым ключом. Криптосистема RSA. Ранцевая криптосистема.	Всего аудиторных часов		
		4		2
		Онлайн		

6 - 8	Криптографические протоколы. Протокол выработки общего сек-ретного ключа. Протоколы электронной цифровой подписи. Про-токолы аутентификации удаленных абонентов. Протоколы доказа-тельства с нулевым разглашением знаний. Протоколы разделения секрета.	Всего аудиторных часов		
		6		3
		Онлайн		
9-16	**Защита информации от случайных деструктивных воздействий**	16		8
9	Цифровые деньги. Структура централизованной платежной систе-мы. Жизненный цикл цифровой купюры.	Всего аудиторных часов		
		2		1
		Онлайн		
10 - 11	Стохастические методы защиты информации. Теория, применение и оценка качества генераторов псевдослучайных чисел (ГПСЧ). Внесение неопределенности в работу средств и объектов защиты. Функции ГПСЧ и хеш-генераторов в системах ОБИ.	Всего аудиторных часов		
		4		2
		Онлайн		
12	Разрушающие программные воздействия (РПВ). Структура ком-плекса программных средств антивирусной защиты. Методы анти-вирусной защиты.	Всего аудиторных часов		
		2		1
		Онлайн		
13	Контроль целостности информации. CRC-коды. Криптографиче-ские методы контроля целостности информации.	Всего аудиторных часов		
		2		1
		Онлайн		
14 - 16	Разграничение доступа. Организация парольных систем.	Всего аудиторных часов		
		6		3
		Онлайн		

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	1 Семестр
	ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ РАБОТ

	Работа 1. Криптоанализ шифра "Усложненная перестановка по таблице". Работа 2. Протоколы электронной цифровой подписи. Работа 3. Российский стандарт криптозащиты ГОСТ 28147-89. Работа 4. Американский стандарт криптозащиты AES.
4 - 5	Работа 1. Криптоанализ шифра "Усложненная перестановка по таблице".
5 - 7	Работа 2. Протоколы электронной цифровой подписи.
8 - 9	Работа 3. Российский стандарт криптозащиты ГОСТ 28147-89.
10 - 11	Работа 4. Американский стандарт криптозащиты AES.

5. 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 по адресу http://dozen.mephi.ru.

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.

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)**
ОПК-1	З-ОПК-1	Э, КИ-8, КИ-16
	У-ОПК-1	Э, КИ-8, КИ-16
	В-ОПК-1	Э, КИ-8, КИ-16
ОПК-2	З-ОПК-2	Э, КИ-8, КИ-16
	У-ОПК-2	Э, КИ-8, КИ-16
	В-ОПК-2	Э, КИ-8, КИ-16
ОПК-3	З-ОПК-3	Э, КИ-8, КИ-16
	У-ОПК-3	Э, КИ-8, КИ-16
	В-ОПК-3	Э, КИ-8, КИ-16
ОПК-4	З-ОПК-4	Э, КИ-8, КИ-16

	У-ОПК-4	Э, КИ-8, КИ-16
	В-ОПК-4	Э, КИ-8, КИ-16
ОПК-5	З-ОПК-5	Э, КИ-8, КИ-16
	У-ОПК-5	Э, КИ-8, КИ-16
	В-ОПК-5	Э, КИ-8, КИ-16
ОПК-6	З-ОПК-6	Э, КИ-8, КИ-16
	У-ОПК-6	Э, КИ-8, КИ-16
	В-ОПК-6	Э, КИ-8, КИ-16
ОПК-7	З-ОПК-7	Э, КИ-8, КИ-16
	У-ОПК-7	Э, КИ-8, КИ-16
	В-ОПК-7	Э, КИ-8, КИ-16
ОПК-8	З-ОПК-8	Э, КИ-8, КИ-16
	У-ОПК-8	Э, КИ-8, КИ-16
	В-ОПК-8	Э, КИ-8, КИ-16
ПК-1	З-ПК-1	Э, КИ-8, КИ-16
	У-ПК-1	Э, КИ-8, КИ-16
	В-ПК-1	Э, КИ-8, КИ-16
ПК-2	З-ПК-2	Э, КИ-8, КИ-16
	У-ПК-2	Э, КИ-8, КИ-16
	В-ПК-2	Э, КИ-8, КИ-16
ПК-3	З-ПК-3	Э, КИ-8, КИ-16
	У-ПК-3	Э, КИ-8, КИ-16
	В-ПК-3	Э, КИ-8, КИ-16
ПК-4	З-ПК-4	Э, КИ-8, КИ-16
	У-ПК-4	Э, КИ-8, КИ-16
	В-ПК-4	Э, КИ-8, КИ-16
УК-4	З-УК-4	Э, КИ-8, КИ-16
	У-УК-4	Э, КИ-8, КИ-16
	В-УК-4	Э, КИ-8, КИ-16
УКЦ-1	З-УКЦ-1	Э, КИ-8, КИ-16
	У-УКЦ-1	Э, КИ-8, КИ-16
	В-УКЦ-1	Э, КИ-8, КИ-16
УКЦ-2	З-УКЦ-2	Э, КИ-8, КИ-16
	У-УКЦ-2	Э, КИ-8, КИ-16
	В-УКЦ-2	Э, КИ-8, КИ-16

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*»		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.

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, Москва: НИЯУ МИФИ, 2012

2. ЭИ Ч-45 Применение искусственных нейронных сетей и системы остаточных классов в криптографии : учебное пособие, Москва: Физматлит, 2012

3. 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 П64 Поточные шифры : , А.В.Асосков [и др.], М.: Кудиц-образ, 2003

3. 004 Ш76 Секреты и ложь : Безопасность данных в цифровом мире, Б. Шнайер, М.и др.: Питер, 2003

4. 004 Г82 Цифровая стеганография : , В. Г. Грибунин, И. Н. Оков, И. В. Туринцев, М.: Солон-Пресс, 2002

5. 0 М24 Современная криптография : теория и практика, В. Мао, Москва [и др.]: Вильямс, 2005

6. 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

7. 004 И20 Теория, применение и оценка качества генераторов псевдослучайных последовательностей : , М.А. Иванов, И.В. Чугунков, Москва: Кудиц-образ, 2003

8. 0 В24 Введение в криптографию : Новые математические дисциплины, Под ред. В.В. Ященко, СПб и др.: МЦНМО; Питер, 2001

9. 519 С13 Введение в алгебраические коды : учебное пособие, Ю. Л. Сагалович, Москва: ИППИ, 2010

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

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 (при его наличии)

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.

4. 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.

10. 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 (при его наличии)

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.