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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ КРИПТОГРАФИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
3	2	72	16	0	16		40	0	З
4	2	72	20	0	20		32	0	ЗО
Итого	4	144	36	0	36	0	72	0	

АННОТАЦИЯ

Курс включает в себя основную информацию, необходимую для построения и конфигурации Инфраструктуры Открытых ключей в рамках того или иного предприятия. Рассматриваются достоинства и недостатки различных моделей доверия Удостоверяющих центров. В рамках курса студенты знакомятся с нормативно-правовыми актами, регламентирующими использование средств криптографической защиты информации (СКЗИ). Вторая половина курса нацелена на формирование практических навыков разработки компонентов Инфраструктуры Открытых ключей и включает в себя знакомство студентов с криптографическими средствами, предоставляемыми операционными системами семейства Windows, в частности CryptoAPI.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение принципов, методов и средств построения компонентов Инфраструктуры Открытых ключей (ИОК).

В курсе рассматриваются следующие темы:

- принципы построения Инфраструктуры Открытых ключей,
- модели доверия при построении архитектуры Удостоверяющих Центров,
- основные стандарты в сфере использования Инфраструктуры Открытых ключей,
- понятие электронной подписи, нормативно-правовые акты, регламентирующие использование электронной подписи,
- разработка прикладного криптографического ПО с использованием MS CryptoAPI,
- регистрация событий, связанных с безопасностью.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные в результате освоения учебной дисциплины знания, умения, навыки используются в процессе дипломного проектирования.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**

научно-исследовательский			
выполнение научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных	методы обеспечения безопасности данных	ПК-4.2 [1] - Способен участвовать в выполнении научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных *Основание:* Профессиональный стандарт: 06.032	З-ПК-4.2[1] - Знать: методы обеспечения безопасности данных; У-ПК-4.2[1] - Уметь: применять методы обеспечения безопасности данных; В-ПК-4.2[1] - Владеть: навыками выполнения научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных
проектный			
разработка проектных решений по обеспечению безопасности данных с применением криптографических методов	информационные ресурсы	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети);

			методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа.; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее.; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных

			систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.

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
	3 Семестр						
1	Первый раздел	1-8	8/0/8		25	КИ-8	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-2, У-ПК-2, В-ПК-2
2	Второй раздел	9-16	8/0/8		25	КИ-16	З-ПК-4.2, У-ПК-4.2,

							В-ПК-4.2, З-ПК-2, У-ПК-2, В-ПК-2
	Итого за 3 Семестр		16/0/16		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4.2, У-ПК-4.2, В-ПК-4.2
	4 Семестр						
1	Первый раздел	1-4	10/0/10		25	КИ-4	В-ПК-2, З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-2, У-ПК-2
2	Второй раздел	5-8	10/0/10		25	КИ-8	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-2, У-ПК-2, В-ПК-2
	Итого за 4 Семестр		20/0/20		50		
	Контрольные мероприятия за 4 Семестр				50	ЗО	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2

* – 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**
ЗО	Зачет с оценкой
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	3 Семестр	16	0	16
1-8	**Первый раздел**	8	0	8
1 - 2	**Введение в ИОК** Инфраструктура открытых ключей. Компоненты инфраструктуры открытых ключей. Функции инфраструктуры открытых ключей. Понятие доверия. Криптографические ключи. Жизненный цикл ключа.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0

	Сертификат ключа подписи. Жизненный цикл сертификата ключа подписи			
3 - 4	**Удостоверяющие центры** Понятия удостоверяющего центра. Функции удостоверяющего центра. Политика сертификата. Регламент удостоверяющего центра. Основные типы архитектуры ИОК. Архитектура индивидуального УЦ. Архитектура единичного УЦ. Иерархическая архитектура подчиненных УЦ. Гибридная архитектура УЦ. Кросс-сертифицированные корпоративные УЦ.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
5 - 6	**Стандарты в области ИОК** Основные стандарты в области инфраструктуры открытых ключей. Нотация ASN.1. Форматы кодирования ASN.1. Формат кодирования BER. Формат кодирования CER. Формат кодирования DER. Стандарт X.509. Назначение стандарта X.509. Основные поля сертификата в соответствии со спецификацией X.509. Семейство стандартов PKCS. Стандарт PKCS #7. Стандарт запросов на сертификат PKCS #10. Стандарт контейнеров обмена личной информацией PKCS #12.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
7 - 8	**Аккредитация УЦ** Аккредитованный Удостоверяющий Центр. Процедура аккредитации Удостоверяющего Центра. Законодательные акты, регламентирующие работу Аккредитованных Удостоверяющих центров.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
9-16	**Второй раздел**	8	0	8
9 - 12	**Электронная подпись** Определение электронной подписи. Принцип работы электронной подписи. Функции электронной подписи. ФЗ-63 «Об электронной подписи. Виды электронной подписи. Простая электронная подпись. Неквалифицированная электронная подпись. Квалифицированная электронная подпись. Средства электронной подписи. Требования к средствам электронной подписи. Квалифицированный сертификат электронной подписи. Требования, предъявляемые к квалифицированному сертификату электронной подписи. Регламент выдачи квалифицированного сертификата электронной подписи.	Всего аудиторных часов		
		4	0	4
		Онлайн		
		0	0	0
13 - 16	**Форматы электронной подписи.** Форматы электронной подписи. Формат подписи CMS. Принцип создания подписи в формате CMS. Область применения формата электронной подписи CMS. Формат подписи CAdES. Типы подписи CAdES. Формат подписи CAdES-BES. Формат подписи CAdES-T. Формат подписи CAdES-C. Форматы подписи CAdES-X. Формат подписи CAdES-A. Формат подписи XMLDSig. Структура подписи в формате XMLDSig. Элементы подписи XMLDSig.	Всего аудиторных часов		
		4	0	4
		Онлайн		
		0	0	0
	4 Семестр	20	0	20
1-4	**Первый раздел**	10	0	10
1 - 4	**Программный интерфейс MS CryptoAPI** Криптопровайдер. Понятие криптопровайдера. Функции криптопровайдера в ОС Windows. Программный	Всего аудиторных часов		
		10	0	10
		Онлайн		

	интерфейс приложений MS CryptoAPI. Архитектура интерфейса MS CrytoAPI ОС семейства Windows. Функции работы с криптопровайдерами. Функции работы с криптографическими ключами. Импорт/экспорт криптографических ключей. Функции работы с криптографическими сообщениями. Функции шифрования/создания подписи.	0	0	0
5-8	**Второй раздел**	10	0	10
5 - 6	**Использование MS CryptoAPI в среде Microsoft .NET** Криптографические средства Microsoft .NET. Криптографическая библиотека классов Microsoft .NET. Пространство имен System.Security.Cryptography. Иерархия классов криптографической библиотеки Microsoft .NET. Абстрактный класс SymmetricAlgorithm. Абстрактный класс AsymetricAlgorithm. Реализации известный криптографических алгоритмов в среде Microsoft .NET.	Всего аудиторных часов		
		8	0	8
		Онлайн		
		0	0	0
7 - 8	**Работа с COM-объектом CertEnroll** Certificate Enrollment API. COM-объект Microsoft CertEnroll. Объект CX509Enrollment. Объект CX500DistinguishedName. Объект CX509CertificateRequestPKCS10. Объект CX509PrivateKey.	Всего аудиторных часов		
		2	0	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**
	3 Семестр
	Л/Р 1 работа с Microsoft УЦ с применением криптопровайдера КриптоПро CSP
	Л/Р 2 установка и настройка комплекса КриптоПро УЦ 2.0
	Л/Р 3 управляющие сертификаты
	Л/Р 4 Практическое применение PKI
	4 Семестр
	Л/Р 1 Работа с криптопровайдерами

	Л/Р 2 Работа с ключевыми контейнерами
	Л/Р 3 Работа с криптографическими сообщениями
	Л/Р 4 Работа с функциями cryptoapi для работы с сертификатами

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, влючают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятиий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы, работа с коспьютерными программами.

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)**	**Аттестационное мероприятие (КП 2)**
ПК-2	З-ПК-2	З, КИ-8, КИ-16	КИ-4, КИ-8
	У-ПК-2	З, КИ-8, КИ-16	КИ-4, КИ-8
	В-ПК-2	З, КИ-8, КИ-16	КИ-4, КИ-8
ПК-4.2	З-ПК-4.2	З, КИ-8, КИ-16	ЗО, КИ-4, КИ-8
	У-ПК-4.2	З, КИ-8, КИ-16	ЗО, КИ-4, КИ-8
	В-ПК-4.2	З, КИ-8, КИ-16	ЗО, КИ-4, КИ-8

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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций и семинарских занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время семинарских занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

При необходимости в конце лекции преподаватель оставляет время для того, чтобы студенты имели возможность задать вопросы по изучаемому материалу.

Лекции нацелены на освещение основополагающих положений теории алгоритмов и теории функций алгебры логики, наиболее трудных вопросов, как правило, связанных с доказательством необходимых утверждений и теорем, призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого семинара.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе лекций, аудиторных практических занятий, лабораторных и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции. В лекционном курсе главное место отводится общетеоретическим проблемам.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Смирнов Павел Владимирович, к.т.н.