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 № УМС-575/01-1

от 30.08.2021 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	3	108	20	0	20		14-32	0	Э
Итого	5	180	36	0	36	0	54-72	0	

Москва, 2020

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**

организационно-управленческий			
организовать эффективную работу по криптографической защите информационных ресурсов организации	информационные ресурсы	ПК-4.3 [1] - способен организовать эффективную работу по криптографической защите информационных ресурсов организации *Основание:* Профессиональный стандарт: 06.032	З-ПК-4.3[1] - Знать: криптографические методы обеспечения безопасности информации; У-ПК-4.3[1] - Уметь: организовать эффективную работу по криптографической защите информационных ресурсов организации; В-ПК-4.3[1] - Владеть: навыками организации эффективной работы по криптографической защите информационных ресурсов организации
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 иди 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.
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

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			25	КИ-8	З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4.2, У-ПК-4.2, В-ПК-4.2
2	Второй раздел	9-16			25	КИ-16	З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4.2, У-ПК-4.2, В-

							ПК-4.2
	Итого за 3 Семестр		16/0/16		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, 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			25	КИ-4	З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4.2, У-ПК-4.2, В-ПК-4.2
2	Второй раздел	5-8			25	КИ-8	З-ПК-4.3, У-ПК-

							4.3, В-ПК-4.3, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4.2, У-ПК-4.2, В-ПК-4.2
	Итого за 4 Семестр		20/0/20		50		
	Контрольные мероприятия за 4 Семестр				50	Э	З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, З-ПК-2, У-ПК-2, В-ПК-2, 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**
КИ	Контроль по итогам
З	Зачет

Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	3 Семестр	16	0	16
1-8	**Первый раздел**	8		8
1 - 2	**Введение в ИОК** Инфраструктура открытых ключей. Компоненты инфраструктуры открытых ключей. Функции инфраструктуры открытых ключей. Понятие доверия. Криптографические ключи. Жизненный цикл ключа. Сертификат ключа подписи. Жизненный цикл сертификата ключа подписи	Всего аудиторных часов 2 Онлайн		
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 Онлайн		4
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 Онлайн		
7 - 8	**Аккредитация УЦ** Аккредитованный Удостоверяющий Центр. Процедура аккредитации Удостоверяющего Центра. Законодательные акты, регламентирующие работу Аккредитованных Удостоверяющих центров.	Всего аудиторных часов 2 Онлайн		4
9-16	**Второй раздел**	8		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 Онлайн		4

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		4
		Онлайн		
	4 Семестр	20	0	20
1-4	**Первый раздел**	10		10
1 - 4	**Программный интерфейс MS CryptoAPI** Криптопровайдер. Понятие криптопровайдера. Функции криптопровайдера в ОС Windows. Программный 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.	Всего аудиторных часов		
		10		10
		Онлайн		
5-8	**Второй раздел**	10		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		8
		Онлайн		
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		2
		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

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основными образовательными технологиями в освоении дисциплин профессионального цикла являются традиционные технологии лекций и лабораторных работ. Интерактивные методики обеспечиваются решением индивидуальных задач студентами и коллективным обсуждением результатов и методов решения.

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	Э, КИ-4, КИ-8
	У-ПК-2	З, КИ-8, КИ-16	Э, КИ-4, КИ-8
	В-ПК-2	З, КИ-8, КИ-16	Э, КИ-4, КИ-8
ПК-4.2	З-ПК-4.2	З, КИ-8, КИ-16	Э, КИ-4, КИ-8
	У-ПК-4.2	З, КИ-8, КИ-16	Э, КИ-4, КИ-8
	В-ПК-4.2	З, КИ-8, КИ-16	Э, КИ-4, КИ-8
ПК-4.3	З-ПК-4.3	З, КИ-8, КИ-16	Э, КИ-4, КИ-8
	У-ПК-4.3	З, КИ-8, КИ-16	Э, КИ-4, КИ-8
	В-ПК-4.3	З, КИ-8, КИ-16	Э, 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
75-84		C	
70-74		D	

			существенных неточностей в ответе на вопрос.
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. 004 М 21 Комментарии к Доктрине информационной безопасности Российской Федерации. : , Москва: Горячая линия -Телеком, 2018

2. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Москва: Горячая линия -Телеком, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

приложены

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

приложены

Автор(ы):

Смирнов Павел Владимирович, к.т.н.