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

АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

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
1	3	108	64	0	0		8	0	Э
Итого	3	108	64	0	0	0	8	0	

АННОТАЦИЯ

Цель дисциплины – формирование у студентов знаний о современных асимметричных криптосистемах и особенностях их применения при комплексной защите объектов информатизации.

В курсе рассматриваются следующие темы:

- основные понятия и задачи криптографии с открытым ключом;
- основные типы криптографических алгоритмов с открытым ключом;
- основные методы построения и оценки качества протоколов на основе криптосистем с открытым ключом.
- типовые методы криптографического анализа и оценивания криптографической стойкости;
- проблемы и методы управления ключевым материалом асимметричных криптосистем;
- принятые отечественные, зарубежные и международные стандарты для асимметричных криптосистем и рекомендации по их использованию;
- тенденции развития и основных направлений исследований в области асимметричных криптосистем;
- вопросы лицензирования и сертификации средств криптографической защиты информации;
- параметры безопасности для основных используемых на практике типов асимметричных криптосистем;

Знания и практические навыки, полученные в курсе «Криптографические методы защиты информации», используются при изучении других дисциплин профессионального цикла, а также при выполнении курсовых и дипломных работ.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – формирование у студентов знаний о современных асимметричных криптосистемах и особенностях их применения при комплексной защите объектов информатизации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Цель дисциплины – формирование у студентов знаний о современных асимметричных криптосистемах и особенностях их применения при комплексной защите объектов информатизации.

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**
проектный			
разработка проектных решений по обеспечению безопасности данных с применением криптографических методов	информационные ресурсы	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные

			стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению

			безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
научно-исследовательский			
выполнение научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных	методы обеспечения безопасности данных	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.032	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие

			требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

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	Первый раздел	1-8	32/0/0		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-3, У-ПК-3, В-ПК-3
2	Второй раздел	9-16	32/0/0		25	КИ-16	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-3, У-ПК-3, В-ПК-3

	Итого за 1 Семестр		64/0/0		50		
	Контрольные мероприятия за 1 Семестр				50	Э	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-3, У-ПК-3, В-ПК-3

* – 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	64	0	0
1-8	**Первый раздел**	32	0	0
1	**Введение** Криптографические примитивы и криптографические протоколы по защите информации. Классификация примитивов с открытым ключом. Синонимы: асимметричные, двухключевые, с открытым ключом криптосистемы. Плюсы и минусы асимметричных криптосистем.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
2	**Необходимые сведения из алгебры и теории чисел** Теория делимости в кольце целых чисел и многочленов. Евклидовы кольца. Наибольший общий делитель и наименьшее общее кратное. Расширенный алгоритм Евклида и его сложность. Простые числа. Попарно взаимно простые числа. Китайская теорема об остатках. Функция Эйлера и ее свойства. Теорема Эйлера – Ферма - Кармайкла. Псевдопростые числа. Вероятностные и детерминированные методы нахождения простых целых чисел. Метод нахождения простых чисел в стандарте ГОСТ 34.10-94. Сведение сравнений n-ой степени по произвольному модулю к системе сравнений по попарно взаимно простым модулям, к сравнениям по примарному и простому модулю. Сравнения первой и второй степени. Символы Лежандра и Якоби. Критерий Эйлера. Метод Берлекемпа решения сравнений второй степени по простому модулю. Теорема эквивалентности Рабина. Основные факты об эллиптических кривых над полями. Эллиптические кривые и факторизация больших целых	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0

	чисел. Дискретный логарифм в группе точек эллиптической кривой над полем.			
3 - 4	**Основные понятия криптографии с открытым ключом** Предпосылки появления криптографии с открытым ключом. История создания криптографии с открытым ключом. Необходимые сведения из теории сложности вычислений. Однонаправленные (односторонние) функции. Примеры однонаправленных функций. Функции на основе блочных шифров. Однонаправленные функции, основанные на сложности задачи дискретного логарифмирования в различных алгебраических группах. Однонаправленные (односторонние) функции с секретом и их применение для цели шифрования информации. Понятия о цифровой подписи на основе однонаправленной функции с секретом. Открытое распределение ключей. Схема Меркля.	Всего аудиторных часов 8 Онлайн 0	 0 0	 0 0
5 - 6	**Схемы шифрования с открытым ключом** Основные принципы построения. Требования к энтропии открытого текста. Схема открытого шифрования RSA. Методы ускорения реализации. Варианты схемы RSA с малыми CRT-экспонентами. Атаки на схему RSA (атака Винера, Бонеха - Дурфи, и др.). Требования к выбору параметров схемы RSA. Схема RSA-OAEP. Схема открытого шифрования Рабина. Теорема Рабина о сложности решения сравнения 2-й степени по составному модулю. Выбор параметров схемы Рабина. Схема Вильямса. Схемы открытого шифрования Эль Гамаля, Дамгарда. Схема шифрования Крамера - Шоупа. Криптосистемы, основанные на теории кодирования. Введение в коды Гоппы. Общая задача декодирования линейных кодов. Криптосистема открытого шифрования Мак-Элиса. Схема Нидеррайтера. Криптосистемы, основанные на задаче о рюкзаке. Криптосистема открытого шифрования Меркля-Хеллмана и атаки на нее. Алгебраические решетки. L^3 – атака. Криптосистема открытого шифрования Кора - Райвеста. Выбор параметров. Использование в криптографии парных отображений (paiping based crypto).	Всего аудиторных часов 8 Онлайн 0	 0 0	 0 0
7 - 8	**Асимметричные схемы цифровой подписи** Основные понятия. Классификация схем цифровой подписи. Классификация атак на схемы цифровой подписи. Подписание документов с метками времени. Неотрицание авторства и цифровые подписи. Сферы применения цифровых подписей. Схемы цифровой подписи RSA и Рабина. Схема RSA-PSS. Стандарты PKCS. Схема цифровой подписи Эль Гамаля и ее модификации. Атаки на схему в случае некорректной реализации алгоритма. Схема Шнорра. Схема цифровой подписи	Всего аудиторных часов 8 Онлайн 0	 0 0	 0 0

	Крамера - Шоупа. Способы ускорения процедур подписи и проверки. Стандарты цифровой подписи США (FIPS PUB 186) и России (ГОСТ Р 34.10). Методы генерации секретных параметров для стандартов цифровой подписи. Схемы подписи Фиата-Шамира, Файге-Фиата-Шамира и др. Реализация схем цифровой подписи на интеллектуальных карточках. Скрытый канал в схемах цифровой подписи. Схемы совместного шифрования с подписью (Signcryption).Нормативно правовые аспекты использования цифровой подписи.			
9-16	**Второй раздел**	32	0	0
9 - 11	**Разновидности схем цифровой подписи** Подпись вслепую (blind signature) и ее применения. Схемы конфиденциальной подписи (undeniable signature) и их применение. Схемы Шаума. Схемы мультиподписи (multisignature scheme). Групповая подпись (group signature scheme). Схемы подписи с восстановлением сообщения (message recovery). Подпись по доверенности (proxy signature). Подписи с обнаружением подделки (fail-stop digital signature). Подписи, подтверждаемые доверенным лицом (designated confirmer signature). Кольцевая подпись (ring signature).	Всего аудиторных часов 12 Онлайн 0	0 0	0 0
12	**Криптографические функции хэширования** Классификация. Функции хэширования без ключа и с ключом. Слабые и сильные функции хэширования. Атаки на функции хэширования. Парадокс «дней рождений» и хэш-функции. Принципы построения. Функции хеширования на базе симметричных блочных алгоритмов. Функции хэширования Райвеста (MD2, MD4, MD5) и их анализ. Американский стандарт функции хэширования FIPS PUB 180 (SHS) и его изменения (SHS-1, SHS-224, SHS-256, SHS-384, SHS-512). Российские стандарты функции хэширования (ГОСТ Р 34.11). Применение функции хэширования в схемах цифровой подписи и при построении криптосистем. Коды проверки подлинности сообщений (MAC). MAC на основе однонаправленной функции. MAC на основе поточного шифра	Всего аудиторных часов 8 Онлайн 0	0 0	0 0
13 - 15	**Асимметричные схемы пост-квантовой криптографии** Криптосистемы, основанные на хэш-функциях (Gravity-SPHINCS; SPHINCS+); Криптосистемы, основанные на алгебраических кодах (BIG QUAKE; BIKE; Classic McEliece; DAGS; HQC; LAKE; LEDAkem; LEDApkc; Lepton; LOCKER; McNie; NTS-KEM; Ouroboros-R; pqsigRM; QC-MDPC KEM; RaCoSS; RankSign; RLCE-KEM; RQC); Криптосистемы, основанные на алгебраических решётках (CRYSTALS-DILITHIUM; DRS; FALCON; LAC; LIMA; NTRUEncrypt; pqNTRUSign; NTRU-HRSS-KEM; NTRU Prime; Odd Manhattan; qTESLA; Titanium); Криптосистемы, основанные на многомерных системах	Всего аудиторных часов 8 Онлайн 0	0 0	0 0

	(DME; DualModeMS; GeMSS; HiMQ-3; LUOV; MQDSS; Rainbow); Криптосистемы, основанные на изогениях суперсингулярных эллиптических кривых (SIKE (SIDH)).			
16	**Облегченные (легковесные, сбалансированные, низкоресурсные) асимметричные схемы** История появления. Международные стандарты. ISO/IEC 29192-1:2012 Information technology - Security techniques - Lightweight cryptography - Part 1: General. ISO/IEC 29192-4:2013 - Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques. ISO/IEC 29192-5:2016 - Lightweight cryptography - Part 5: Hash-functions.	Всего аудиторных часов		
		4	0	0
		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

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.

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)**
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-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

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:

1. 004 М 21 Глобальная культура кибербезопасности : , Малюк А.А., Москва: Горячая линия - Телеком, 2018

2. ЭИ А 18 Дискретная математика. Модулярная алгебра, криптография, кодирование : , Авдошин С. М., Набебин А. А., Москва: ДМК Пресс, 2017

3. ЭИ Н 62 Методы защиты информации. Шифрование данных : учебное пособие, Никифоров С. Н., Санкт-Петербург: Лань, 2022

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. ЭИ А 28 Основы классической криптологии: секреты шифров и кодов : , Адаменко М. В., Москва: ДМК Пресс, 2016

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):

Варфоломеев Александр Алексеевич, к.ф.-м.н., с.н.с.