

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Анатольевна

Должность: и.о. декана факультета математики и компьютерных наук имени

профессора Н.И. Червякова

Дата подписания: 17.06.2026 16:06:56

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего
образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

И.о. декана факультета математики
и компьютерных наук имени

профессора Н.И. Червякова

Т.А. Грובה

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Аутентификация в киберфизических системах

Направление подготовки

Направленность (профиль)

Год начала обучения

Форма обучения

Реализуется в семестре

10.04.01 Информационная безопасность

Информационная безопасность

киберфизических систем

2026

очная

3

Разработано

Доцент кафедры организации и
технологии защиты информации

к.т.н., доцент Рачков В.Е.

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Аутентификация в киберфизических системах» является формирование профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем» для осуществления деятельности в области защиты киберфизических систем, а также создания новых объектов киберфизических систем.

Основными задачами дисциплины является теоретическое и практическое освоение основных понятий и методов работы по следующим направлениям:

- методология аутентификации в киберфизических системах;
- особенности аутентификации в киберфизических системах;
- криптографические протоколы аутентификации в киберфизических системах;
- процедуры реализации подписи в киберфизических системах.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Аутентификация в киберфизических системах» (Б1.В.08) относится к дисциплинам части, формируемой участниками образовательных отношений. Её освоение происходит в 3 семестре.

3. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-2 Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	ИД-1 ПК-2 Осуществляет анализ особенностей проектирования и реализации политики безопасности вычислительных сетей в киберфизических системах	Перечисляет и кратко характеризует действующие нормативные акты, методические документы, регламентирующие проектирование политик безопасности для вычислительных сетей в составе киберфизических систем
	ИД-2 ПК-2 Проектирует и реализует политики безопасности вычислительных сетей в киберфизических системах	Разрабатывает концептуальную модель политики безопасности для заданной вычислительной сети киберфизической системы (определяет субъекты, объекты, правила разграничения доступа)
	ИД-4 К-2 формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизических системах	Разрабатывает комплект документов политики безопасности для заданной киберфизической системы (положение о политике безопасности, матрица доступа, правила разграничения доступа, инструкции для администраторов)

ПК-3. Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	ИД-1 ПК-3 состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	Перечисляет и кратко характеризует основные нормативные документы, определяющие требования к системе управления информационной безопасностью киберфизических систем
	ИД-2 ПК-3 анализ уязвимости и построение модели угроз для киберфизических систем	Составляет проект документа с предложениями по совершенствованию системы управления информационной безопасностью в соответствии с принятыми в организации шаблонами
	ИД-6 ПК-3 Формализует методологию разработки предложений при совершенствовании системы управления информационной безопасностью киберфизических систем	Готовит развёрнутое заключение по итогам анализа системы управления информационной безопасностью, содержащее ранжированный перечень предложений с указанием ожидаемых результатов и сроков реализации

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: 4 з. е. 144 акад. ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	36
Лабораторных работ/из них практическая подготовка	36
Практических занятий/из них практическая подготовка	-
Самостоятельная работа	36
Формы контроля	
Экзамен	36

* Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий (если иное не установлено образовательным стандартом)

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Форма текущего контроля успеваемости
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические	Лабораторные работы		
1	Методология аутентификации в киберфизических системах Реализация процедуры групповой подписи BBS на билинейных отображениях Реализация процедуры групповой подписи на базе динамической схемы ED-BBS	ИД-1 _{ПК-2} , ИД-2 _{ПК-2} , ИД-4 _{ПК-2} , ИД-1 _{ПК-3} , ИД-2 _{ПК-3} , ИД-6 _{ПК-3}	10.00	-	10.00	8.00	
2	Особенности аутентификации в киберфизических системах Реализация процедуры групповой подписи BBS с отзывом права подписи Построение схемы групповой подписи на решетках по протоколу DKV	ИД-1 _{ПК-2} , ИД-2 _{ПК-2} , ИД-4 _{ПК-2} , ИД-1 _{ПК-3} , ИД-2 _{ПК-3} , ИД-6 _{ПК-3}	10.00	-	10.00	8.00	
3	Процедуры реализации подписи в киберфизических системах Построение схемы групповой подписи на решетках по протоколу LLLS Построение схемы групповой подписи на решетках с процедурой отзыва по протоколу DKV-DVLR Построение схемы групповой подписи на решетках с процедурой отзыва по протоколу LLLS-VLR	ИД-1 _{ПК-2} , ИД-2 _{ПК-2} , ИД-4 _{ПК-2} , ИД-1 _{ПК-3} , ИД-2 _{ПК-3} , ИД-6 _{ПК-3}	8.00	-	8.00	10.00	

4	Криптографические протоколы аутентификации в киберфизических системах Построение криптографического протокола на основе аутсорс-алгоритмов вычисления билинейного отображения Построение криптографического протокола на основе аутсорс-алгоритмов вычисления билинейного отображения	ИД-1 _{ПК-2} , ИД-2 _{ПК-2} , ИД-4 _{ПК-2} , ИД-1 _{ПК-3} , ИД-2 _{ПК-3} , ИД-6 _{ПК-3}	8.00	-	8.00	10.00	
	Итого за 3 семестр		36.00	-	36.00	36.00	
	ИТОГО		36.00	-	36.00	36.00	

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) по дисциплине базируется на перечне осваиваемых компетенций с указанием индикаторов. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины.

Описание шкалы оценивания

Рейтинговой системы оценивания не предусмотрена. Оценивание осуществляется по 5-ти балльной шкале в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента не предусмотрена. Оценивание осуществляется по 5-ти балльной шкале

Промежуточная аттестация в форме экзамена в 3 семестре.

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически завершённый раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Лабораторные занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

8.1.1. Перечень основной литературы:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.

2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.

3. Nayan M. Kakoty, Rupam Goswami, Ramana Vinjamuri, Introduction to Embedded Systems and Robotics : A Practical Guide, Springer, 2024

8.1.2. Перечень дополнительной литературы:

1. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. Астайкина А.И. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли.; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)
9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей: учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск: Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/>
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС«Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрация презентационных мультимедийных материалов, программное обеспечение для проведения веб-конференции.

При проведении практических занятий используются информационно-справочные системы, интерактивная доска для совместной работы команд и сервис для совместной работы.

При реализации дисциплины с применением электронного обучения и дистанционных образовательных технологий материал может размещаться в системе электронного обучения.

Для обеспечения удаленного доступа, в том числе в случае применения электронного обучения, дистанционных образовательных технологий, используется программное обеспечение для проведения веб-конференции, виртуализации рабочих столов и система электронного обучения.

Программное обеспечение:

1	Интерактивная онлайн-доска для совместной работы команд https://workspace.vk.ru/
2	Открытое программное обеспечение для проведения веб-конференции МТС Линк https://mts-link.ru/
3	Платформа для создания онлайн-курсов https://el.ncfu.ru/
4	Российский пакет офисных приложений Р7-Офис https://r7-office.ru/
5	Сервис для совместной работы TEAMLY https://teamly.ru/
6	Альт виртуализация https://www.basealt.ru/alt-virtualization

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	Государственный реестр сертифицированных средств защиты информации https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00
2	Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/588-perechen-ispitatelnykh-laboratorij-n-ross-ru-0001-01bi00
3	Реестр операторов, осуществляющих обработку персональных данных https://pd.rkn.gov.ru/operators-registry/operators-list/
4	Common Vulnerabilities and Exposures/ База данных общеизвестных уязвимостей информационной безопасности https://cve.mitre.org/
5	MITRE ATT&CK® база знаний о тактике и методах противника https://attack.mitre.org/

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия	Учебная аудитория на 30 посадочных мест для проведения занятий лекционного типа, оснащенная оборудованием и техническими средствами обучения: доска магнитно-маркерная, проектор, компьютер с необходимым комплектом лицензионного программного обеспечения.
--------------------	--

Лабораторные занятия	Учебная аудитория на 15 посадочных мест, оснащенная средствами вычислительной техники, обеспечивающая практическую подготовку в соответствии с направленностью (профилем) программы магистратуры «Информационная безопасность киберфизических систем». Лаборатория на 15 посадочных мест, в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации, в том числе, отечественного производства.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой в количестве 10 комплектов с подключением к сети «Интернет» с необходимым комплектом лицензионного программного обеспечения и доступом в электронную информационно-образовательную среду университета.

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения. Специализированная мебель и технические средства обучения, служащие для представления учебной информации.

Материально-техническая база обеспечивает проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, научно-исследовательской работы обучающихся (переносной ноутбук, переносной проектор, компьютеры с необходимым программным обеспечением и выходом в интернет).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

11. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

- 1) для лиц с ограниченными возможностями здоровья по зрению:
 - присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),
 - письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,

- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
- индивидуальное равномерное освещение не менее 300 люкс,
- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются: способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование); ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется

открытый доступ через информационно-телекоммуникационную сеть «Интернет»; для синхронного обучения - время проведения онлайн-занятий и преподаватели; для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнауки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.