

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
СТАРООСКОЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ ИМ. А.А. УГАРОВА
 (филиал) федерального государственного автономного образовательного учреждения
 высшего образования
 «Национальный исследовательский технологический университет «МИСИС»
СТИ НИТУ «МИСИС»

Рабочая программа утверждена
 решением Ученого совета
 СТИ НИТУ «МИСИС»
 от «23» июня 2026 г.
 протокол № 38

Аннотация рабочей программы дисциплины

Информационная безопасность

Кафедра автоматизированных и информационных систем управления им.

Закреплена за кафедрой	<u>Ю.И.Еременко</u>
Направление подготовки	09.03.02 Информационные системы и технологии
Профиль	Информационные системы и технологии
Квалификация	<u>Бакалавр</u>
Форма обучения	<u>Очная</u>
Общая трудоемкость	3 ЗЕТ

Часов по учебному плану	144
в том числе:	
аудиторные занятия	51
самостоятельная работа	57
часов на контроль	36

Формы контроля в семестрах:
 экзамен 7, курсовая работа 8

Распределение часов дисциплины по семестрам

Семестр	7		8		Итого	
	УП	РП	УП	РП	УП	РП
Лекции	17	17	-	-	17	17
Лабораторные	17	17	-	-	17	17
Практические	17	17	-	-	17	17
Контактная работа	51	51	-	-	51	51
Сам. работа	21	21	36	36	57	57
Часы на контроль	36	36	-	-	36	36
Итого	108	108	36	36	144	144

Год набора 2026г.

ЦЕЛИ ОСВОЕНИЯ	
Цель дисциплины – формирование теоретических знаний в области управления информационными ресурсами систем и сетей и отработка умений и навыков использования инструментальных программных систем, сетевых служб и оборудования для защиты информации в компьютерных системах. Задачи дисциплины: • Научить обучающихся основным терминам и понятиям защиты информации; • Научить обучающихся применять теоретические знания в области защиты информации для решения конкретных практических задач по выбранному направлению подготовки; • Научить обучающихся основным угрозам защиты информации и способам их предотвращения; • Научить обучающихся разбираться в типовых атаках направленных на ИС и программные продукты; • Научить обучающихся основным видам криптографических алгоритмов и их уязвимостей	

ИНДИКАТОРЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ, СОВМЕЩЕННЫЕ С РЕЗУЛЬТАТАМИ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ	
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, умение анализировать процессы и системы с использованием соответствующих аналитических, вычислительных и экспериментальных методов, применять системный подход для решения поставленных задач	
Знать:	УК-1-31– Знать основные понятия и термины, связанные с информационной безопасностью; УК-1-32 –Знать основные виды угроз информационной безопасности;
Уметь:	УК-1-У1 – Уметь определять и классифицировать угрозы и атаки.
Владеть:	УК-1-В1 – Владеть навыками обнаружения уязвимостей веб-ресурсов
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	
Знать:	ОПК-3-31– Знать нормативную и законодательную базу в области информационной безопасности
Уметь:	ОПК-3-У1 – Уметь проводить анализ защищенности информационных объектов в различных сферах деятельности человека;
Владеть:	ОПК-3-В1– Владеть навыками реализации поиска потенциально компрометирующей информации в интернете
ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	
Знать:	ОПК-2-31– Знать современное программное обеспечение для защиты информации
Уметь:	ОПК-2-У1 – Уметь проводить анализ работы программ защиты информации
Владеть:	ОПК-2-В1– Владеть навыками развертывания систем защиты информации
ПК-1 Способен участвовать в работах по: - доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных технологий; - поддержанию работоспособности информационных систем и технологий в заданных функциональных характеристиках и в соответствии с критериями качества; - управлению программно-аппаратными средствами информационных служб инфокоммуникационной системы организации; - обеспечению безопасности и целостности данных информационных систем и технологий, а также условий жизненного цикла информационных систем; - адаптации приложений к изменяющимся условиям функционирования; - администрированию сетевой подсистемы инфокоммуникационной системы организации. Использовать технологии разработки объектов профессиональной деятельности в различных областях.	
Знать:	ПК-1-31 – Знать механизмы аутентификации и идентификации при доступе к информационным ресурсам; ПК-1-32 – Знать основные криптографические алгоритмы; ПК-1-33- Знать основные веб-уязвимости и веб-атаки
Уметь:	ПК-1-У1 – Уметь проводить анализ устойчивости различных криптографических алгоритмов ПК-1-У2 – Уметь проводить анализ устойчивости хешей паролей пользователей
Владеть:	ПК-1-В1 – Владеть навыками реализации различных криптографических алгоритмов ПК-1-В2– Владеть навыками реализации различных хэш-функций и электронно-цифровых подписей ПК-1-В3– Владеть навыками реализации защиты от веб-угроз