МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

03.03.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФОРЕНЗИКА

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9, 10

Магнитогорск
2021 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
19.02.2021, протокол № 9

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
03.03.2021 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Михайлова

Рецензент:
начальник отдела информационной безопасности «КУБ» (АО) ,

_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Форензика является неотъемлемой частью комплексной деятельности по обеспечению информационной безопасности. Расследование киберпреступлений и производство экспертиз по ним осложняется постоянным развитием информационных технологий. Целью освоения дисциплины является изучение экспертных методик компьютерной криминалистики и отработка их на практических занятиях.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Форензика входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Анализ рисков информационной безопасности

Анализ уязвимостей программного обеспечения

Производственная - практика по получению профессиональных умений и опыта профессиональной деятельности

Разработка систем защиты информации автоматизированных систем

Безопасность операционных систем

Защита информации от утечки по техническим каналам

Методы выявления нарушений информационной безопасности

Безопасность систем баз данных

Безопасность сетей ЭВМ

Моделирование угроз информационной безопасности

Виртуальные сети

Физические основы передачи информации

Программно-аппаратные средства обеспечения информационной безопасности

Информационные технологии. Базы данных

Безопасность Интернета вещей

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Форензика» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	
ОПК-13.1	Организовывает тестирование систем защиты информации автоматизированных систем
ОПК-13.2	Проводит диагностику систем защиты информации автоматизированных систем
ОПК-13.3	Анализирует уязвимости автоматизированных систем и их систем защиты

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 9 зачетных единиц 324 акад. часов, в том числе:

– контактная работа – 180,9 акад. часов:
– аудиторная – 175 акад. часов;
– внеаудиторная – 5,9 акад. часов;
– самостоятельная работа – 107,4 акад. часов;
– в форме практической подготовки – 0 акад. час;
– подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен, зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Компьютерно техническая экспертиза (КТЭ)								
1.1 Понятия судебная экспертиза и КТЭ. Требования законодательства к методике и методам производства	9	12	14/10И		25	Подготовка к практическому занятию; работа с ЭБС и нормативными документами;	Тестирование	ОПК-13.1
1.2 Классификация методик и построение модели методики производства КТЭ. Базовые критерии.		12	20/8,9И		28,1	Подготовка к практическому занятию; работа с ЭБС и нормативными документами;	Индивидуальное задание	ОПК-13.1, ОПК-13.2, ОПК-13.3
1.3 Применение методов КТЭ. Оценка трудозатрат при производстве комплексной экспертизы.		12	20		30	Подготовка к практическому занятию; работа с ЭБС и нормативными документами;	Индивидуальное задание	ОПК-13.1, ОПК-13.2, ОПК-13.3
1.4 Подготовка к зачету					5	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; Подготовка к зачету	Зачет	ОПК-13.1, ОПК-13.2, ОПК-13.3
Итого по разделу		36	54/18,9И		88,1			
Итого за семестр		36	54/18,9И		88,1		зачёт	
2. Унифицированная методика производства КТЭ								

2.1 Стадии КТЭ. Формирование экспертного заключения.	10	12	20/10И		5,3	Подготовка к практическому занятию; работа с ЭБС и нормативными документами;	Индивидуальное задание	ОПК-13.1, ОПК-13.2, ОПК-13.3
2.2 Применение методик для решения практических задач из профессиональной области.		12	20/7,85И		10	Подготовка к практическому занятию; работа с ЭБС и нормативными документами;	Индивидуальное задание	ОПК-13.1, ОПК-13.2, ОПК-13.3
2.3 Применение инструментов Kali Linux для сбора информации о системе и анализа ее уязвимостей.		10	11		4	Подготовка к практическому занятию; работа с ЭБС и нормативными документами;	Индивидуальное задание	ОПК-13.1, ОПК-13.2, ОПК-13.3
2.4 Подготовка к экзамену						Подготовка к практическому занятию; работа с ЭБС и нормативными документами; Подготовка к экзамену	Экзамен	ОПК-13.1, ОПК-13.2, ОПК-13.3
Итого по разделу		34	51/17,85И		19,3			
Итого за семестр		34	51/17,85И		19,3		экзамен	
Итого по дисциплине		70	105/36, 75И		107,4		экзамен, зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

a) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

b) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

c) Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);

d) Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;

e) Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

f) Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) Разделно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Разделно-компетентностной технологии:

a) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:

a) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ

ошибок, совместный поиск вариантов рационального решения проблемы.

b) Методы IT – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Форензика» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает выполнение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

7 Оценочные средства для проведения промежуточной аттестации

Оценочные средства
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;
ОПК-13.1 Организовывает тестирование систем защиты информации автоматизированных систем
1. Порядок реагирования на компьютерные атаки; 2. Жизненный цикл атаки; 3. Методики разведки и сбора данных для проведения атаки; 4. Методы организации обнаружения атак; 5. Подходы к организации киберразведки; 6. Решить задачу по определению вида атаки по заданным параметрам.
ОПК-13.2 Проводит диагностику систем защиты информации автоматизированных систем
1. Методы организации защиты от атак; 2. Подходы к расследованию инцидентов информационной безопасности; 3. Реализовать разработанную политику сетевой безопасности для заданной конфигурации корпоративной сетевой инфраструктуры. 4. Составить план реагирования на заданный вид атаки;
ОПК-13.3 Анализирует уязвимости автоматизированных систем и их систем защиты
1. Управление уязвимостями; 2. Методы охоты на пользовательские реквизиты; 3. Провести анализ уязвимостей для заданной конфигурации корпоративной сетевой инфраструктуры;

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Внуков, А.А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772(дата обращения: 24.02.2020).

б) Дополнительная литература:

1. Брюхомицкий, Ю.А. Искусственные иммунные системы в информационной безопасности: учебное пособие / Ю. А. Брюхомицкий; Южный федеральный университет. - Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2019. - 147 с. - ISBN 978-5-9275-3212-4. - Текст: электронный. - URL: https://new.znanium.com/catalog/product/1088177 (дата обращения: 26.02.2020)

2. Веселов, Г.Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог: Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст: электронный. - URL: https://new.znanium.com/catalog/product/997108 (дата обращения: 26.02.2020)

5. Сетевая защита информации. Лабораторный практикум: учебное пособие [для вузов] / Д. Н. Мазнин [и др.]; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск: МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 22.10.2019). – Макрообъект*. - ISBN 978-5-9967-1605-0. - Текст: электронный. - Сведения доступны также на CD-ROM.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта*.
4. *При открытии макрообъектов учитывайте настройки антивирусной защиты.

в) Методические указания:

1. Методические указания по выполнению лабораторных работ (Приложение 1)
2. Методические указания по выполнению внеаудиторных самостоятельных работ (Приложение 2)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
Oracle Virtual Box	свободно распространяемое ПО	бессрочно
Anaconda Python	свободно распространяемое ПО	бессрочно
WordPress	свободно распространяемое ПО	бессрочно
NotePad++	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
СЗИ Страж NT в.3	К-271-12 от 16.10.2012	бессрочно

СКЗИ КриптоПро CSP	К-271-12 от 16.10.2012	бессрочно
VIP Net Client	Д-946-14 от 22.07.2014	бессрочно
VIP Net CryptoService	Д-946-14 от 22.07.2014	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Double Commander	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Международная реферативная и полнотекстовая справочная база данных научных изданий «Scopus»	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- Мультимедийные средства хранения, передачи и представления информации.

Лаборатория технической защиты информации:

1. АКС-1301 Анализатор спектра
2. Комплекс радиомониторинга "Касандра К6" с диапазоном рабочих частот 0,009-6000Мгц
3. Комплекс радиомониторинга "Касандра К21" с диапазоном рабочих частот 0,009-21000Мгц
4. Генератор шума стационарный "ГШ-1000-М"
5. Система виброакустической и акустической защиты "Соната-АВ"
6. Устройство защиты телефонных переговоров от прослушивания и записи "Прокруст-200"
7. Портативный поисковый комплекс амплитудной пеленгации «Касандра С6»
8. Система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) Сигурд

Компьютерные классы:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для самостоятельной работы обучающихся:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.